Management Software

AT-S63

Web Browser Interface User's Guide

AT-S63 Version 2.2.0 for the AT-9400 Layer 2+ Switches
AT-S63 Version 3.0.0 for the AT-9400 Basic Layer 3 Switches

PN 613-50592-00 Rev G

Allied Telesis™

Copyright © 2007 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface 15
How This Guide is Organized 16
Product Documentation 18
Where to Go First 19
Starting a Management Session 20
Document Conventions 21
Where to Find Web-based Guides 22
Contacting Allied Telesis 23
Online Support 23
Email and Telephone Support 23
Warranty 23
Returning Products 23
Sales or Corporate Information 23
Management Software Updates 23

Section I: Basic Operations 25

Chapter 1: Basic Switch Parameters 27
Configuring the Switch's Name, Location, and Contact 28
Changing the Manager and Operator Passwords 30
Setting the System Date and Time 32
Rebooting a Switch 35
Pinging a Remote System 36
Returning the AT-S63 Management Software to the Factory Default Values 37
Displaying the IP Address of the Local Interface 39
Displaying System Information 40

Chapter 2: Port Parameters 43
Configuring Port Parameters 44
Displaying Port Parameters 51
Displaying Port Statistics 53
Resetting a Port to the Default Settings 56

Chapter 3: Enhanced Stacking 57
Setting a Switch's Enhanced Stacking Status 58
Selecting a Switch in an Enhanced Stack 60
Returning to the Master Switch 62
Displaying the Enhanced Stacking Status 63

Chapter 4: SNMPv1 and SNMPv2c 65
Enabling or Disabling SNMP Management 66
Creating a New SNMPv1 and SNMPv2c Community 68
Modifying an SNMPv1 and SNMPv2c Community 71
Deleting an SNMPv1 and SNMPv2c Community 72
Displaying the SNMPv1 and SNMPv2c Communities 73

Chapter 5: MAC Address Table 75
Displaying the MAC Address Table 76
Adding Static Unicast and Multicast MAC Addresses 79
Deleting Unicast and Multicast MAC Addresses 81
Deleting All Dynamic MAC Addresses 82
Changing the Aging Time 83

Chapter 6: Static Port Trunks 85
Creating a Static Port Trunk 86
Modifying a Static Port Trunk 90
Deleting a Port Trunk 92
Displaying the Port Trunks 93

Chapter 7: Port Mirroring 95
Creating a Port Mirror 96
Modifying a Port Mirror 99
Disabling a Port Mirror 100
Deleting a Port Mirror 101
Displaying the Port Mirror 102

Section II: Advanced Operations 103

Chapter 8: File System 105
Listing the Files in Flash Memory or on a Compact Flash Card 106
Selecting an Active Boot Configuration File 109

Chapter 9: File Downloads and Uploads 111
Downloading a File 112
Uploading a File 116

Chapter 10: Event Logs and Syslog Client 119
Working with the Event Logs 120
Enabling or Disabling the Event Logs 120
Displaying Events 122
Clearing an Event Log 126
Modifying the Event Log Full Action 127
Saving an Event Log to a File 128
Working with Syslog Output Definitions 129
Configuring a Syslog Output Definition 129
Viewing a Syslog Output Definition 132
Modifying a Syslog Output Definition 132
Deleting a Syslog Output Definition 133

Chapter 11: Classifiers 135
Configuring a Classifier 136
Modifying a Classifier 142
Deleting a Classifier 144
Displaying the Classifiers 145

Chapter 12: Access Control Lists 147
Configuring an Access Control List 148
Modifying an Access Control List 151
Deleting an Access Control List 152
Displaying the Access Control Lists 153

Chapter 13: Class of Service 155
Configuring CoS 156
Mapping CoS Priorities to Egress Queues 158
Configuring Egress Scheduling 160
Displaying the CoS Settings 161
Displaying the QoS Schedule 163

Chapter 14: Quality of Service 165
Managing Flow Groups 166
Configuring a Flow Group 166
Modifying a Flow Group 169
Deleting a Flow Group 170
Displaying the Flow Groups 170
Managing Traffic Classes 172
Configuring a Traffic Class 172
Modifying a Traffic Class 176
Deleting a Traffic Class 178
Displaying the Traffic Classes 178
Managing Policies 180
Configuring a Policy 180
Modifying a Policy 183
Deleting a Policy 184
Deleting all Flow Groups, Traffic Classes, and Policies 185
Displaying Policies 185

Chapter 15: Denial of Service Defenses 187
Configuring Denial of Service Defense 188
Displaying the DoS Settings 191

Chapter 16: IGMP Snooping 193
Configuring IGMP Snooping 194
Displaying a List of Host Nodes 197
Displaying a List of Multicast Routers 199

Section III: SNMPv3 201

Chapter 17: SNMPv3 203
Configuring the SNMPv3 Protocol 204
Enabling or Disabling SNMP Management 205
Configuring the SNMPv3 User Table 208
Creating a User Table Entry 208
Deleting a User Table Entry 211
Modifying a User Table Entry 212
Configuring the SNMPv3 View Table 216
Creating a View Table Entry 216
Deleting a View Table Entry 219
Modifying a View Table Entry 219
Configuring the SNMPv3 Access Table 222
Creating an Access Table 222
Deleting an Access Table Entry 225
Modifying an Access Table Entry 226
Configuring the SNMPv3 SecurityToGroup Table 229
Creating a SecurityToGroup Table Entry 229
Deleting a SecurityToGroup Table Entry 232
Modifying a SecurityToGroup Table Entry 232

Configuring the SNMPv3 Notify Table 235
Creating a Notify Table Entry 235
Deleting a Notify Table Entry 237
Modifying a Notify Table Entry 238
Configuring the SNMPv3 Target Address Table 240
Creating a Target Address Table Entry 240
Deleting a Target Address Table Entry 243
Modifying Target Address Table Entry 244
Configuring the SNMPv3 Target Parameters Table 247
Creating a Target Parameters Table Entry 247
Deleting a Target Parameters Table Entry 250
Modifying a Target Parameters Table Entry 251
Configuring the SNMPv3 Community Table 254
Creating an SNMPv3 Community Table Entry 254
Deleting an SNMPv3 Community Table Entry 257
Modifying an SNMPv3 Community Table Entry 257
Displaying SNMPv3 Tables 260
Displaying User Table Entries 260
Displaying View Table Entries 262
Displaying Access Table Entries 263
Displaying SecurityToGroup Table Entries 264
Displaying Notify Table Entries 265
Displaying Target Address Table Entries 266
Displaying Target Parameters Table Entries 267
Displaying SNMPv3 Community Table Entries 268

Section IV: Spanning Tree Protocols 271

Chapter 18: Spanning Tree and Rapid Spanning Tree Protocols 273
Enabling or Disabling a Spanning Tree Protocol 274
Configuring STP 276
Configuring STP Bridge Settings 276
Configuring STP Port Settings 279
Displaying the STP Settings 280
Resetting STP to the Default Settings 282
Configuring RSTP 284
Configuring RSTP Bridge Settings 284
Configuring RSTP Port Settings 287
Displaying RSTP Settings 288
Resetting RSTP to the Default Settings 291

Chapter 19: Multiple Spanning Tree Protocol 293
Enabling MSTP 294
Configuring MSTP 296
Configuring MSTP Parameters 296
Configuring the CIST Priority 299
Managing MSTIs 300
Creating an MSTI 300
Modifying an MSTI 301
Deleting an MSTI 302
Configuring MSTP Port Parameters 304
Displaying the MSTP Configuration 308
Resetting MSTP to the Default Settings 313

Section V: Virtual LANs 315

Chapter 20: Port-based and Tagged VLANs 317
Creating a New Port-Based or Tagged VLAN 318
Modifying a VLAN 323
Deleting a VLAN 325
Selecting a VLAN Mode 326
Displaying VLANs 327

Chapter 21: GARP VLAN Registration Protocol 331
Configuring GVRP 332
Enabling or Disabling GVRP on a Port 334
Displaying the GVRP Configuration 335
Displaying the GVRP Port Configuration 336
Displaying the GVRP Database 337
Displaying the GVRP State Machine 338
Displaying the GVRP Counters 341
Displaying the GIP Connected Ports Ring 344

Section VI: Port Security 345

Chapter 22: MAC Address-based Port Security 347
Configuring Port Security 348
Displaying Port Security Levels 351

Chapter 23: 802.1x Port-based Network Access Control 353
Setting Port Roles 354
Enabling or Disabling 802.1x Port-based Network Access Control 356
Configuring Authenticator Port Parameters 357
Configuring Supplicant Port Parameters 363
Displaying the Port-based Network Access Control Parameters 365
Displaying the Port Status 365
Displaying the Port Settings 367
RADIUS Accounting 369
Configuring RADIUS Accounting 369
Displaying the RADIUS Accounting Settings 370

Section VII: Management Security 371

Chapter 24: Encryption Keys, PKI, and SSL 373
Displaying the Encryption Keys 374
Displaying the PKI Settings and Certificates 376
Displaying the SSL Settings 379

Chapter 25: Secure Shell (SSH) 381
Configuring SSH 382
Displaying the SSH Settings 384

Chapter 26: TACACS+ and RADIUS Protocols 387
Enabling or Disabling TACACS+ or RADIUS 388
Configuring the TACACS+ Client Settings 390
Displaying the TACACS+ Client Settings 392
Configuring the RADIUS Client Settings 394
Displaying the RADIUS Client Settings 396

Chapter 27: Management Access Control List 399
Enabling or Disabling the Management ACL 400
Creating an ACE 402
Modifying an ACE 404
Deleting an ACE 405
Displaying the Management Access Control List 406

Index 407

Figures

Chapter 1: Basic Switch Parameters 27
Figure 1: General Tab (Configuration) 28
Figure 2: System Time Tab 33
Figure 3: Ping Client Tab (Monitoring) 36
Figure 4: System Utilities Tab (Configuration) 38
Figure 5: General Tab (Monitoring) 40

Chapter 2: Port Parameters 43
Figure 6: Port Settings Tab (Configuration) 44
Figure 7: Port Configuration Page 45
Figure 8: Port Settings Tab (Monitoring) 51
Figure 9: Port Status Page 52
Figure 10: Port Statistics Page 53

Chapter 3: Enhanced Stacking 57
Figure 11: Enhanced Stacking Tab (Configuration) 59
Figure 12: Stacking Switches Page 60
Figure 13: Enhanced Stacking Tab (Monitoring) 63

Chapter 4: SNMPv1 and SNMPv2c 65
Figure 14: SNMP Tab (Configuration) 66
Figure 15: SNMPv1 & SNMPv2c Communities Tab 68
Figure 16: Add New SNMPv1 & SNMPv2c Community Page 69
Figure 17: SNMP Tab (Monitoring) 73
Figure 18: SNMPv1 & SNMPv2c Communities Tab (Monitoring) 74

Chapter 5: MAC Address Table 75
Figure 19: MAC Address Tab (Configuration) 76
Figure 20: View MAC Addresses Page 78
Figure 21: Add MAC Address Page 79

Chapter 6: Static Port Trunks 85
Figure 22: Port Trunking Tab (Configuration) 87
Figure 23: Add New Trunk Page 88
Figure 24: Modify Trunk Page 91
Figure 25: Port Trunking Tab (Monitoring) 93

Chapter 7: Port Mirroring 95
Figure 26: Port Mirroring Tab (Configuration) 96
Figure 27: Modify Mirror Page 97
Figure 28: Example of a Modify Mirror Page 98
Figure 29: Port Mirroring Tab (Monitoring) 102

Chapter 8: File System 105
Figure 30: File System Tab (Configuration) 106
Figure 31: Viewing File Page 108

Chapter 9: File Downloads and Uploads 111
Figure 32: System Utilities Tab (Configuration) 114

Chapter 10: Event Logs and Syslog Client 119
Figure 33: Event Log Tab (Configuration) 121
Figure 34: Event Log Example Displayed in Normal Mode 125
Figure 35: Event Log Example Displayed in Full Mode 126
Figure 36: Modifying Event Log Output 1 Window 127
Figure 37: Create Event Log Output Page 130
Figure 38: View Event Log Output Page 132
Figure 39: Modify Event Log Output Page 133

Chapter 11: Classifiers 135
Figure 40: Classifier Tab (Configuration) 136
Figure 41: Create Classifier Page 137
Figure 42: Create Classifier Page - IP Protocol 138
Figure 43: Modify Classifier Page 142
Figure 44: Classifier Tab (Monitoring) 145

Chapter 12: Access Control Lists 147
Figure 45: ACL Tab (Configuration) 148
Figure 46: Create ACLs Page 149
Figure 47: Modify ACLs Page 151
Figure 48: ACL Tab (Monitoring) 153
Figure 49: View ACLs Page 154

Chapter 13: Class of Service 155
Figure 50: CoS Tab (Configuration) 156
Figure 51: CoS Setting for Port Page 157
Figure 52: Queuing & Scheduling Tab (Configuration) 158
Figure 53: CoS Tab (Monitoring) 161
Figure 54: CoS Setting for Port Page 161
Figure 55: QoS Scheduling Tab (Monitoring) 163

Chapter 14: Quality of Service 165
Figure 56: Flow Group Tab (Configuration) 166
Figure 57: Create Flow Group Page 167
Figure 58: Modify Flow Group Page 169
Figure 59: Flow Group Tab (Monitoring) 171
Figure 60: Traffic Class Tab 172
Figure 61: Create Traffic Class Page 173
Figure 62: Modify Traffic Class Page 177
Figure 63: Traffic Class Tab (Monitoring) 178
Figure 64: Policies Tab (Configuration) 180
Figure 65: Create Policy Page 181
Figure 66: Modify Policy Page 184
Figure 67: Policies Tab (Monitoring) 185

Chapter 15: Denial of Service Defenses 187
Figure 68: DoS Tab (Configuration) 188
Figure 69: DoS Configuration for Ports Page 189
Figure 70: DoS Tab (Monitoring) 191
Figure 71: DoS Monitor for Ports Page 192

Chapter 16: IGMP Snooping 193
Figure 72: IGMP Tab (Configuration) 194
Figure 73: IGMP Tab (Monitoring) 197
Figure 74: View Multicast Routers List Page 199

Chapter 17: SNMPv3 203
Figure 75: SNMP Tab (Configuration) 206
Figure 76: SNMPv3 User Table Tab (Configuration) 209
Figure 77: Add New SNMPv3 User Page 209
Figure 78: Modify SNMPv3 User Page 213
Figure 79: SNMPv3 View Table Tab (Configuration) 217
Figure 80: Add New SNMPv3 View Page 217
Figure 81: Modify SNMPv3 View Page 220
Figure 82: SNMPv3 Access Table Tab (Configuration) 222
Figure 83: Add New SNMPv3 Access Page 223
Figure 84: Modify SNMPv3 Access Page 227
Figure 85: SNMPv3 SecurityToGroup Table Tab (Configuration) 230
Figure 86: Add New SNMPv3 SecurityToGroup Page 230
Figure 87: Modify SNMPv3 SecurityToGroup Page 233
Figure 88: SNMPv3 Notify Table Tab (Configuration) 236
Figure 89: Add New SNMPv3 Notify Page 236
Figure 90: Modify SNMPv3 Notify Page 238
Figure 91: SNMPv3 Target Address Table Tab (Configuration) 241
Figure 92: Add New SNMPv3 Target Address Page 241
Figure 93: Modify SNMPv3 Target Address Page 244
Figure 94: SNMPv3 Target Parameters Table Tab (Configuration) 247
Figure 95: Add New SNMPv3 Target Parameters Page 248
Figure 96: Modify SNMPv3 Target Parameter Page 251
Figure 97: SNMPv3 Community Table Tab (Configuration) 255
Figure 98: Add New SNMPv3 Community Page 255
Figure 99: Modify SNMPv3 Community Page 258
Figure 100: SNMP Tab (Monitoring) 261
Figure 101: SNMPv3 User Table Tab (Monitoring) 262
Figure 102: SNMPv3 View Table Tab (Monitoring) 263
Figure 103: SNMPv3 Access Table Tab (Monitoring) 264
Figure 104: SNMPv3 SecurityToGroup Table Tab (Monitoring) 265
Figure 105: SNMPv3 Notify Table Tab (Monitoring) 266
Figure 106: SNMPv3 Target Address Table Tab (Monitoring) 267
Figure 107: SNMPv3 Target Parameters Table Tab (Monitoring) 268
Figure 108: SNMPv3 Community Table Tab (Monitoring) 269

Chapter 18: Spanning Tree and Rapid Spanning Tree Protocols 273
Figure 109: Spanning Tree Tab (Configuration) 274
Figure 110: Configure STP Parameters Tab (Configuration) 277
Figure 111: STP Settings - Port(s) Page 279
Figure 112: Spanning Tree Tab (Monitoring) 281
Figure 113: Monitor STP Parameters Tab (Monitoring) 281
Figure 114: STP Settings Page 282
Figure 115: Configure RSTP Parameters Tab (Configuration) 285
Figure 116: RSTP Settings - Port(s) Page 287
Figure 117: Monitor RSTP Parameters Tab (Monitoring) 289
Figure 118: RSTP Port Status Page 289
Figure 119: RSTP Settings Page 290

Chapter 19: Multiple Spanning Tree Protocol 293
Figure 120: Spanning Tree Tab (Configuration) 294
Figure 121: Configure MSTP Parameters Tab (Configuration) 297
Figure 122: Add New MSTI Page 300
Figure 123: Modify MSTI Page 302
Figure 124: MSTP Settings - Port(s) Page 304
Figure 125: Monitor MSTP Parameters Tab (Monitoring) 309

Figure 126: MSTP Settings - Port(s) Page 310
Figure 127: MSTP Port Status - Port(s) Page 311

Chapter 20: Port-based and Tagged VLANs 317
Figure 128: VLAN Tab (Configuration) 318
Figure 129: Add New VLAN Page 320
Figure 130: VLAN Tab (Monitoring) 327
Figure 131: View Protected VLAN Page 329

Chapter 21: GARP VLAN Registration Protocol 331
Figure 132: GVRP Tab (Configuration) 332
Figure 133: GVRP Port Configuration Page 334
Figure 134: GVRP Tab (Monitoring) 335
Figure 135: GVRP Port Configuration Page 336
Figure 136: GVRP Database Page 337
Figure 137: GVRP State Machine for VLAN Page 338
Figure 138: GVRP Counters Page 341
Figure 139: GIP Connected Ports Ring Page 344

Chapter 22: MAC Address-based Port Security 347
Figure 140: Port Security Tab (Configuration) 348
Figure 141: Security for Ports Page (Configuration) 348
Figure 142: Port Security Tab (Monitoring) 351
Figure 143: Security for Port(s) Page 351

Chapter 23: 802.1x Port-based Network Access Control 353
Figure 144: 802.1x Port Access Tab (Configuration) 354
Figure 145: Port Role Configuration Page 355
Figure 146: Authenticator Parameters Page 358
Figure 147: Supplicant Parameters Page 363
Figure 148: 802.1x Port Access Tab (Monitoring) 365
Figure 149: Port Access Port Status Page 366
Figure 150: Authenticator Port Parameters Page 367
Figure 151: Supplicant Port Parameters Page 368

Chapter 24: Encryption Keys, PKI, and SSL 373
Figure 152: Keys Tab (Monitoring) 374
Figure 153: PKI Tab (Monitoring) 376
Figure 154: X509 Certificate Details Page 377
Figure 155: SSL Tab (Monitoring) 379

Chapter 25: Secure Shell (SSH) 381
Figure 156: Secure Shell Tab (Configuration) 382
Figure 157: Secure Shell Tab (Monitoring) 384

Chapter 26: TACACS+ and RADIUS Protocols 387
Figure 158: Server-based Authentication Tab (Configuration) 388
Figure 159: TACACS+ Client Configuration Page 390
Figure 160: Server-Based Authentication Tab (Monitoring) 392
Figure 161: TACACS+ Client Configuration Page 393
Figure 162: RADIUS Client Configuration Page 394
Figure 163: RADIUS Client Configuration Page 396

Chapter 27: Management Access Control List 399
Figure 164: Mgmt. ACL Tab (Configuration) 400
Figure 165: Add New MACL Page 402
Figure 166: Modify MACL Page 404
Figure 167: Mgmt. ACL Tab (Monitoring) 406

Tables

Table 1: AT-S63 Software Modules 123
Table 2: Event Severity Levels 125
Table 3: Default Syslog Facilities 131
Table 4: Default Mappings of IEEE 802.1p Priority Levels to Egress Priority Queues 159
Table 5: Bridge Priority Value Increments 278
Table 6: Port Priority Value Increments 280
Table 7: MSTP Auto Update Port Internal Path Costs 305
Table 8: MSTP Auto Update Port Trunk Internal Path Costs 305
Table 9: MSTP Auto External Path Costs 306
Table 10: MSTP Auto External Path Trunk Costs 307
Table 11: GVRP State Machine Parameters 338
Table 12: GVRP Counters 341

Preface

This guide contains instructions on how to manage the AT-9400 Layer 2+ and Basic Layer 3 Gigabit Ethernet Switches from the web browser interface in the AT-S63 Management Software.

This preface contains the following sections:

- ❒ “How This Guide is Organized” on page 16
- ❒ “Product Documentation” on page 18
- ❒ “Where to Go First” on page 19
- ❒ “Starting a Management Session” on page 20
- ❒ “Document Conventions” on page 21
- ❒ “Where to Find Web-based Guides” on page 22
- ❒ “Contacting Allied Telesis” on page 23

Note
The web browser interface does not support all the management functions of the AT-9400 Switch. Those management tasks not supported by this interface can be performed from the menus interface or the command line interface.

Caution
The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product’s export status.

How This Guide is Organized

This guide has the following sections and chapters:

- Section I: Basic Operations

  Chapter 1, “Basic Switch Parameters” on page 27

  Chapter 2, “Port Parameters” on page 43

  Chapter 3, “Enhanced Stacking” on page 57

  Chapter 4, “SNMPv1 and SNMPv2c” on page 65

  Chapter 5, “MAC Address Table” on page 75

  Chapter 6, “Static Port Trunks” on page 85

  Chapter 7, “Port Mirroring” on page 95

- Section II: Advanced Operations

  Chapter 8, “File System” on page 105

  Chapter 9, “File Downloads and Uploads” on page 111

  Chapter 10, “Event Logs and Syslog Client” on page 119

  Chapter 11, “Classifiers” on page 135

  Chapter 12, “Access Control Lists” on page 147

  Chapter 13, “Class of Service” on page 155

  Chapter 14, “Quality of Service” on page 165

  Chapter 15, “Denial of Service Defenses” on page 187

  Chapter 16, “IGMP Snooping” on page 193

- Section III: SNMPv3

  Chapter 17, “SNMPv3” on page 203

- Section IV: Spanning Tree Protocols

  Chapter 18, “Spanning Tree and Rapid Spanning Tree Protocols” on page 273

  Chapter 19, “Multiple Spanning Tree Protocol” on page 293

- Section V: Virtual LANs

  Chapter 20, “Port-based and Tagged VLANs” on page 317

  Chapter 21, “GARP VLAN Registration Protocol” on page 331

- Section VI: Port Security

  Chapter 22, "MAC Address-based Port Security" on page 347

  Chapter 23, "802.1x Port-based Network Access Control" on page 353

- Section VII: Management Security

  Chapter 24, "Encryption Keys, PKI, and SSL" on page 373

  Chapter 25, "Secure Shell (SSH)" on page 381

  Chapter 26, "TACACS+ and RADIUS Protocols" on page 387

  Chapter 27, "Management Access Control List" on page 399

Product Documentation

For overview information on the features of the AT-9400 Switch and the AT-S63 Management Software, refer to:

- AT-S63 Management Software Features Guide (PN 613-000801)

For instructions on starting a local or remote management session, refer to:

- Starting an AT-S63 Management Session Guide (PN 613-000817)

For instructions on installing or managing a stand-alone switch, refer to:

- AT-9400 Gigabit Ethernet Switch Installation Guide (PN 613-000357)
- AT-S63 Management Software Menus Interface User's Guide (PN 613-50570-00)
- AT-S63 Management Software Command Line Interface User's Guide (PN 613-50571-00)
- AT-S63 Management Software Web Browser Interface User's Guide (PN 613-50592-00)

For instructions on installing or managing a stack of AT-9400 Basic Layer 3 Switches and the AT-StackXG Stacking Module, refer to:

- AT-9400 Stack Installation Guide (PN 613-000796)
- AT-S63 Stack Command Line Interface User's Guide (PN 613-000777)

Where to Go First

Allied Telesis recommends that you read Chapter 1, Overview, in the *AT-S63 Management Software Features Guide* before you begin to manage the switch for the first time. There you will find a variety of basic information about the unit and the management software, like the two levels of manager access levels and the different types of management sessions.

The *AT-S63 Management Software Features Guide* is also your resource for background information on the features of the switch. You can refer there for the relevant concepts and guidelines when you configure a feature for the first time.

Starting a Management Session

For instructions on how to start a local or remote management session on the AT-9400 Switch, refer to the *Starting an AT-S63 Management Session Guide*.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at **www.alliedtelesis.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support section of the Allied Telesis web site: **www.alliedtelesis.com**.

Warranty

The Gigabit Ethernet switches in the AT-9400 Series have a Lifetime Warranty (5 Year Fan and Power Supply Unit). All Allied Telesis warranties are subject to the terms and conditions set out in the Allied Telesis Limited Warranties on our web site at **www.alliedtelesis.com/warranty/default.aspx**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Management Software Updates

New releases of the management software for our managed products are available from the following Internet sites:

- Allied Telesis web site: **www.alliedtelesis.com**
- Allied Telesis FTP server: **ftp://ftp.alliedtelesis.com**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.

Section I

Basic Operations

This section has the following chapters:

- Chapter 1, “Basic Switch Parameters” on page 27
- Chapter 2, “Port Parameters” on page 43
- Chapter 3, “Enhanced Stacking” on page 57
- Chapter 4, “SNMPv1 and SNMPv2c” on page 65
- Chapter 5, “MAC Address Table” on page 75
- Chapter 6, “Static Port Trunks” on page 85
- Chapter 7, “Port Mirroring” on page 95

Chapter 1

Basic Switch Parameters

This chapter contains the following sections:

- “Configuring the Switch’s Name, Location, and Contact” on page 28
- “Changing the Manager and Operator Passwords” on page 30
- “Setting the System Date and Time” on page 32
- “Rebooting a Switch” on page 35
- “Pinging a Remote System” on page 36
- “Returning the AT-S63 Management Software to the Factory Default Values” on page 37
- “Displaying the IP Address of the Local Interface” on page 39
- “Displaying System Information” on page 40

Configuring the Switch's Name, Location, and Contact

This procedure assigns a name to the switch. The name appears at the top of the web browser windows. Names can help you identify your switches when you manage them and avoid performing a configuration procedure on the wrong switch. This procedure also assigns the name of the administrator responsible for maintaining the unit and the location of the switch.

To assign a name, location, and contact to a switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 1.

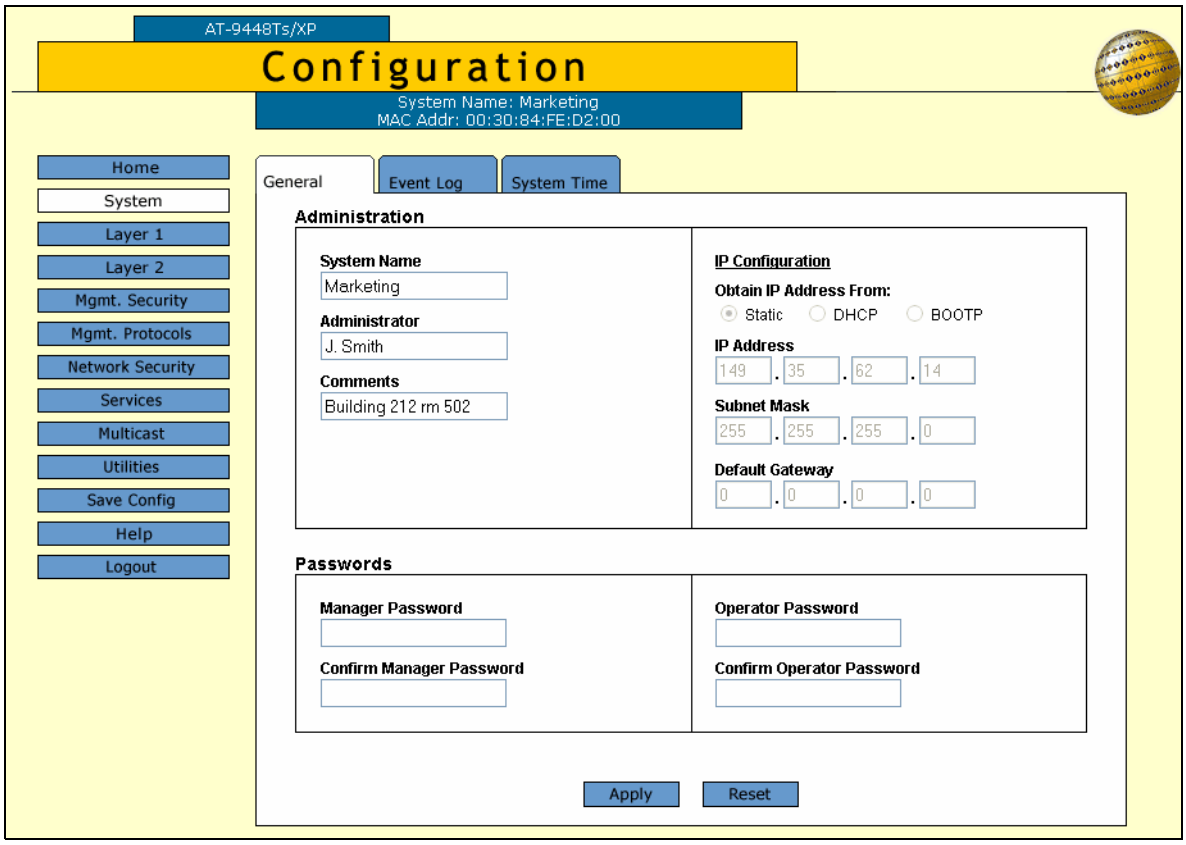

Figure 1. General Tab (Configuration)

Note
This procedure describes the System Name, Administrator, and Comments parameters in the Administration section of the tab. The parameters in the IP Configuration section are described in "Displaying the IP Address of the Local Interface" on page 39. The Passwords section is described in "Changing the Manager and Operator Passwords" on page 30. The Reset button at the bottom of the tab resets the switch and is explained in "Rebooting a Switch" on page 35.

2. Configure the following parameters as necessary:

   System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed at the top of the AT-S63 management pages and tabs. The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.

   Administrator
   This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

   Comments
   This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.

3. Click **Apply** to activate your changes on the switch.

4. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Changing the Manager and Operator Passwords

There are two levels of management access on the AT-9400 Switch: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S63 management session. The default password for manager access is "friend." The default password for operator access is "operator." Passwords are case sensitive.

To change the manager or operator password, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. In the Passwords section, enter the new values. The parameters are described below.

   Manager Password
   Confirm Manager Password
   You use these parameters to change the manager's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend." The password is case sensitive.

   Caution
   Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

   Operator Password
   Confirm Operator Password
   Use these parameters to change the operator's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator." The password is case sensitive.

Caution
Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Note
A change to a password is immediately activated on the switch. You must use the new password the next time you start a management session of the switch.

3. Click **Apply** to activate your change on the switch.
4. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Setting the System Date and Time

This procedure explains how to set the switch's date and time. Setting the date and time is important if you plan to view the events in the switch's event log or send the events to a syslog server. The correct date and time are also important if the management software will be sending traps to a management workstation or if you plan to create a self-signed SSL certificate. Events, traps, and self-signed certificates should contain the date and time of when they occurred or, in the case of certificates, when they were created.

There are two ways to set the switch's date and time. One method is to set it manually. The AT-9400 Switch has an onboard battery that maintains the date and time even when the unit is powered off or reset.

The second method uses the Simple Network Time Protocol (SNTP). The AT-S63 Management Software comes with the client version of this protocol. You can configure the AT-S63 software to obtain the current date and time from an SNTP or Network Time Protocol (NTP) server located on your network or the Internet.

SNTP is a reduced version of the NTP. However, the SNTP client software in the AT-S63 Management Software is interoperable with NTP servers.

Note
In order for the management software on the switch to communicate with an SNTP or NTP server, there must be an interface on the local subnet from where the switch is reaching the server. The switch uses the IP address of the interface as its source address when sending packets to the server. For background information on routing interfaces, refer to the *AT-S63 Management Software Features Guide*.

Note
The default system time on the switch is midnight, January 1, 1980.

To set the system time manually or to configure SNTP client, do the following:

1. From the Home Page, select **Configuration**.
2. Select the **System Time** tab.

The System Time tab is shown in Figure 2.

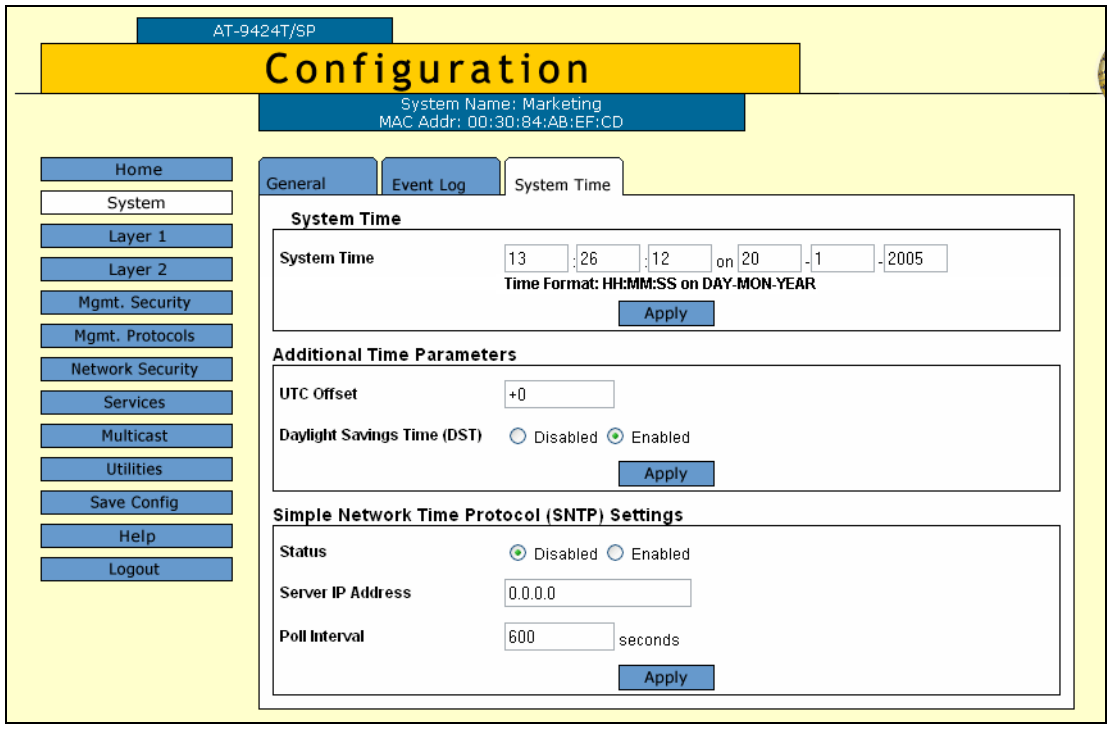

Figure 2. System Time Tab

3. To set the system time manually, do the following:

   a. In the System Time section of the tab, enter the time and date in the following format.

      hh:mm:ss dd-mm-yyyy

   b. Click **Apply**.

4. To configure the switch to obtain its date and time from an SNTP or NTP server on your network or the Internet, configure the following options:

   UTC Offset
   Specifies the difference between the UTC and local time. The default is 0 hours. The range is -12 to +12 hours.

   Note
   If the interface on the local subnet from where the switch is reaching the server is using DHCP to set its IP configuration, it automatically attempts to determine this value. In this case, you do not need to configure a value for the UTC Offset parameter.

Daylight Savings Time (DST)
Enables or disables the system's adjustment for daylight savings time. The default is enabled.

> **Note**
> The switch does not set DST automatically. If the switch is in a locale that uses DST, you must remember to enable this in April when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, this option should be set to disabled all the time.

Status
Enables or disables the SNTP client on the switch. The default is disabled.

Server IP Address
Specifies the IP address of an SNTP server.

> **Note**
> If the local interface on the switch is obtaining its IP address and subnet mask from a DHCP server, you can configure the server to provide the interface with an IP address of an NTP or SNTP server. If you configured the server to provide this address, then you do not need to enter it here.

Poll Interval
Specifies the number of seconds the switch waits between polling the SNTP or NTP server. The default is 600 seconds. The range is from 60 to 1200 seconds.

5. When you finish configuring the parameters, click the **Apply** buttons.

   If you enabled the SNTP client, the switch immediately polls the SNTP or NTP server for the current date and time. (The switch automatically polls the server whenever a change is made to any of the parameters in this menu, so long as SNTP is enabled.)

6. To permanently save your changes, click **Save Config**.

Rebooting a Switch

Note
All unsaved parameters changes are discarded when a system is reset. To save your parameter changes, click the **Save Config** option in the main menu.

To reboot a switch, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Click **Reset** at the bottom of the tab.

   A confirmation prompt is displayed.

3. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

Note
The switch does not forward packets while it initializes the AT-S63 Management Software and loads its active configuration file. This process takes between 20 seconds to 2 minutes to complete, depending on the number and types of commands in the configuration file.

Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Pinging a Remote System

This procedure instructs the switch to ping a node on your network. This can be useful in determining whether an active path exists between the switch and another network device. Note the following before performing this procedure:

> **Note**
> The switch must have a routing interface on the local subnet from where it is pinging the end node. The switch uses the IP address of the interface as its source address when pinging the device. For background information on routing interfaces, refer to the *AT-S63 Management Software Features Guide*.

To instruct the switch to ping a network device, perform the following procedure:

1. From the home page, select **Monitoring**.
2. From the Monitoring menu, select the **Utilities** option.
3. Select the **Ping Client** tab.

   The Ping Client tab is shown in Figure 3.

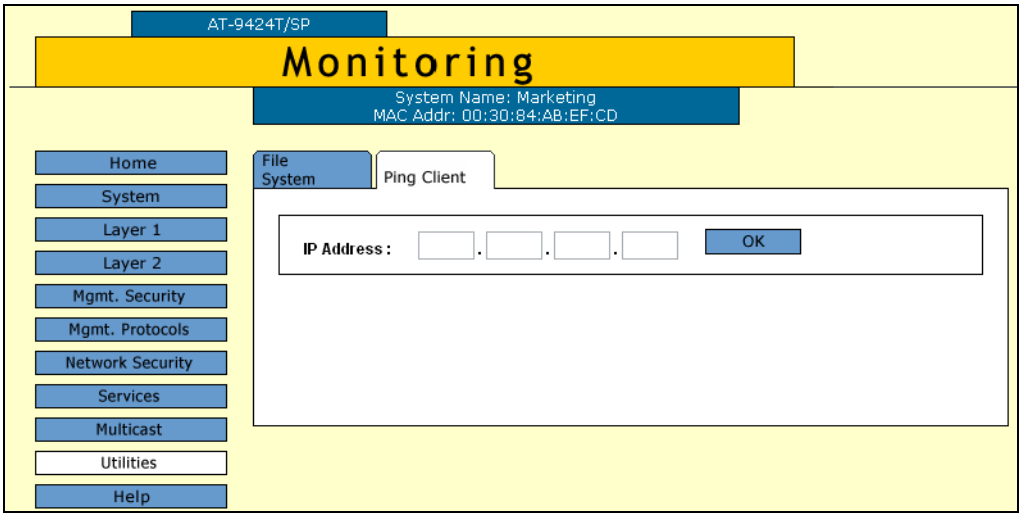

Figure 3. Ping Client Tab (Monitoring)

4. Enter the IP address of the end node to be pinged by the switch.
5. Click **OK**. The results of the ping are displayed in a popup window.
6. To stop the ping, click **OK**.

Returning the AT-S63 Management Software to the Factory Default Values

The procedure in this section returns all AT-S63 Management Software parameters to their default values. Note the following before performing this procedure:

- Returning the switch to its default parameter settings deletes all routing interfaces and port-based and tagged VLANs on the switch.
- Returning the switch to its default parameter settings does not delete files from the switch's file system or encryption keys from the key database. For instructions on how to delete files, refer to the *AT-S63 Management Software Menus Interface User's Guide* or the *AT-S63 Management Software Command Line Interface User's Guide*.
- The speed of the Terminal Port on the switch is not changed.
- Returning a switch to its default values does not alter the contents of the active boot configuration file. To reset the file to the default settings, you must establish a local or remote management session with the switch after it reboots and select Save Config from the menu. Otherwise, the switch reverts back to the previous configuration the next time you reset or power cycle the unit.
- If the switch is an isolated switch (i.e., a switch that is not a part of an enhanced stack) or the master switch of an enhanced stack, it is unlikely you will be able to reestablish your web browser management session at the completion of this procedure, because all routing interfaces are deleted. You must use a local management session to continue managing the switch.

Caution

This procedure involves a switch reset. Some network traffic may be lost while the unit initializes its management software and loads the default configuration settings, a process that takes approximately 20 seconds to complete.

Note

The AT-S63 Management Software default values are listed in Appendix A, "AT-S63 Default Settings" in the *AT-S63 Management Software Features Guide*.

To return the AT-S63 Management Software to the default settings, perform the following procedure:

1. From the home page, select **Configuration**.

2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab selected by default, as shown in Figure 4.

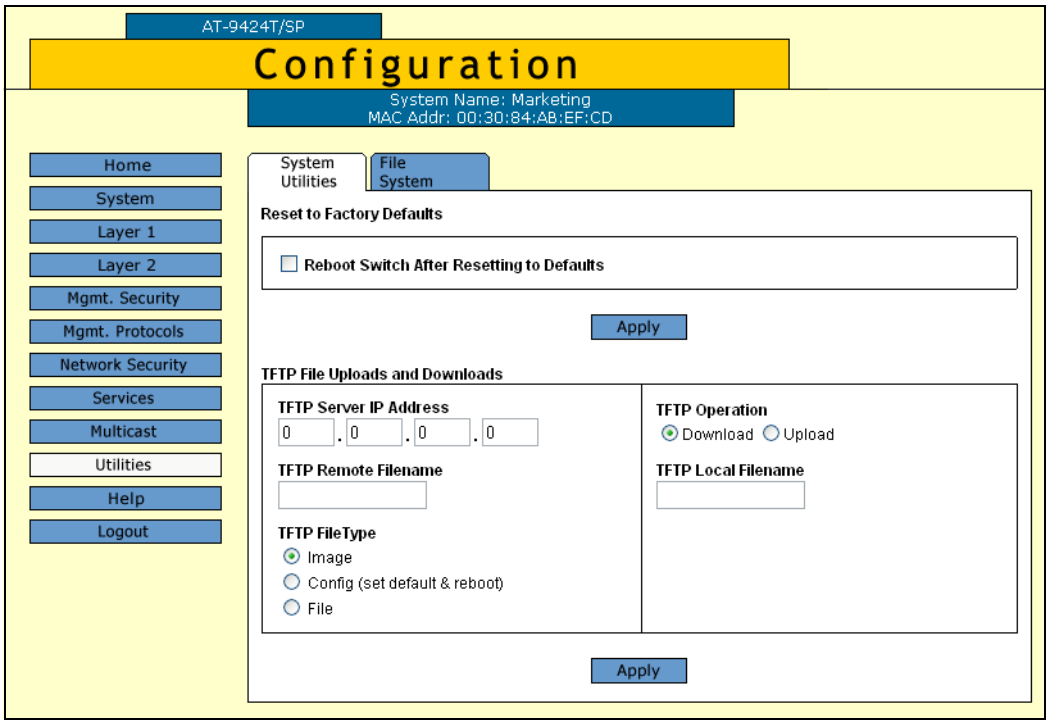

Figure 4. System Utilities Tab (Configuration)

3. Click the **Reboot Switch After Resetting to Defaults** checkbox.

4. Click **Apply**.

   The web browser displays the following prompt:

   ```
   This page may no longer be available while the switch
   reboots. Do you want to continue?
   ```

5. Click **OK** to continue or **Cancel** to cancel the procedure.

   If you select OK, the switch resets and returns all values to the default settings. After the reset is complete, you must establish a new management session if you want to continue managing the unit, probably from a local management session.

   As mentioned at the start of this procedure, returning a switch to is default settings does not alter the contents of the active boot configuration file. To return the file to the default settings, you must save the current switch settings after you establish a new management session with the switch. Otherwise, the switch returns to its previous parameter settings the next time you reset or power cycled the unit.

Displaying the IP Address of the Local Interface

This procedure displays the IP address and subnet mask of the local interface on the switch. The local interface is used for enhanced stacking and remote management of the switch with a Telnet or SSH client, or a web browser. You cannot configure the local interface from the web browser interface, For that, you must use the menus interface or the command line interface.

To view the IP address and subnet mask of the local interface, perform the following procedure:

1. From the home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28. This procedure discusses the parameters in the IP Configuration section of the web page.

   Obtain IP Address from:
   The options in this section indicate the source of the IP address of the local interface. If DHCP or BOOTP is checked, the interface obtained its IP address from a DHCP or BOOTP server on the network. If Static is checked, the IP address was set manually.

   IP Address
   This parameter displays the IP address of the local management interface. This address is either manually assigned to the interface or obtained from a DHCP or BOOTP server.

   Subnet Mask
   This parameter specifies the subnet mask for the interface.

   The IP address and subnet mask fields will be empty if no interface has been designated as the local interface.

   Default Gateway
   For AT-9400 Switches that support IPv4 routing, such as the AT-9424Ts and AT-9448Ts/XP switches, this field displays the IP address of the next hop of the switch's default route. The switch uses the default route when it receives a network packet for routing, but cannot find a route for it in the routing table. This field will contain 0.0.0.0 if no default route is defined on the switch.

   For AT-9400 Switches that do not support IPv4 packet routing, such as the AT-9424T/GB and AT-9424T/SP switches, this field displays the default gateway address. This is the IP address of a router interface on your network. The switch's management software uses this address as the next hop to reaching a remote network device, such as a remote management workstation or a syslog server, when the switch's local interface and the remote device are on different subnets. The default value is 0.0.0.0.

Displaying System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5.

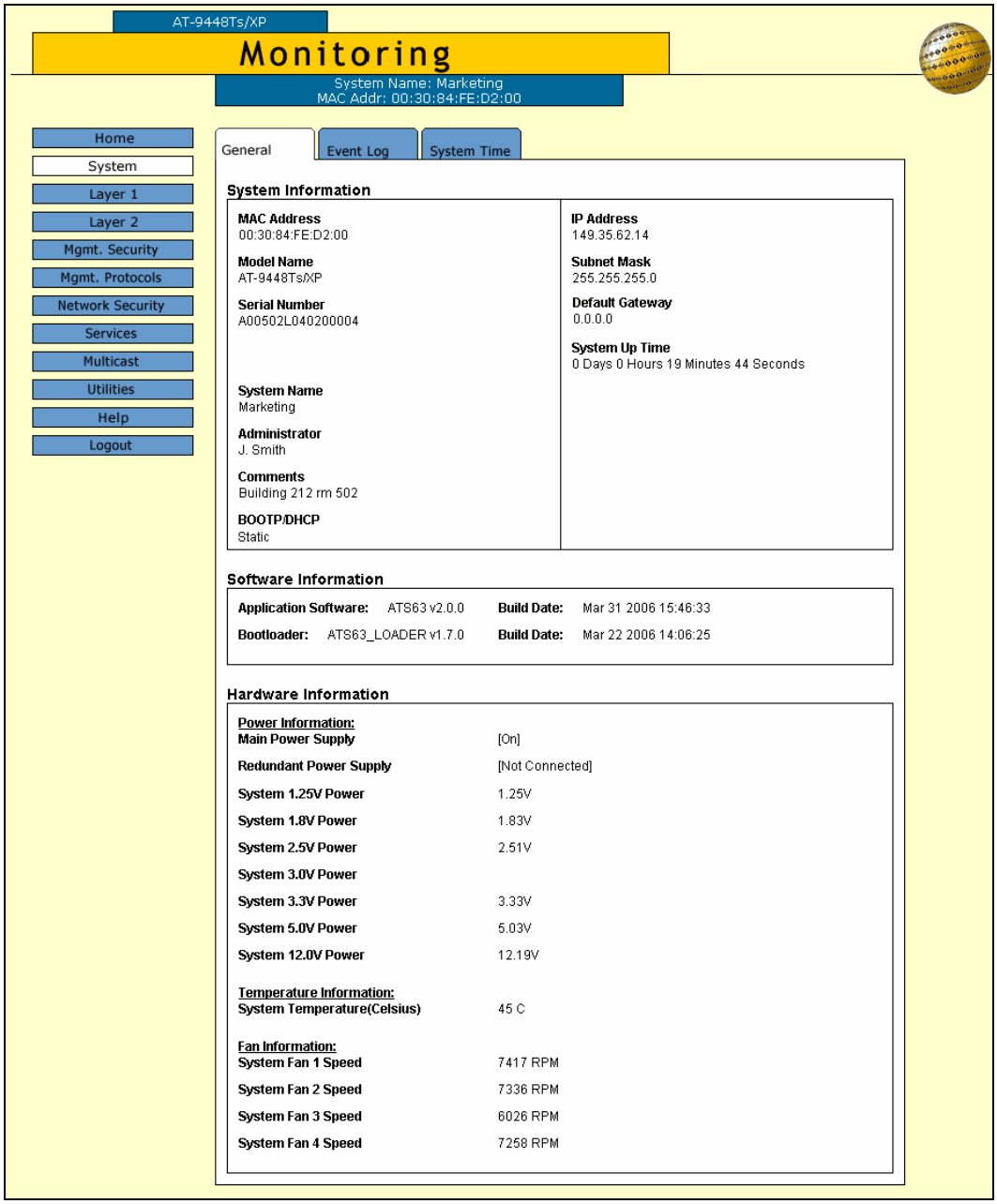

Figure 5. General Tab (Monitoring)

The System Information section displays the following information:

MAC Address
The MAC address of the switch.

Model Name
The model name of the switch.

Serial Number
The serial number of the switch.

System Name
The name of the switch. To set the name, refer to "Configuring the Switch's Name, Location, and Contact" on page 28.

Administrator
The name of the network administrator responsible for managing the switch. To set the name of the administrator, refer to "Configuring the Switch's Name, Location, and Contact" on page 28.

Comments
The location of the switch, (for example, 4th Floor - rm 402B). To set the location, refer to "Configuring the Switch's Name, Location, and Contact" on page 28.

BOOTP/DHCP
The source of the IP address of the local interface. This field will be "DHCP" or "BOOTP" if the local interface obtained its IP configuration from a DHCP or BOOTP server. Alternatively, if the IP address was set manually, this field will be "Static." This field will be blank if the switch does not have a local interface.

IP Address
The IP address of the local interface.

Subnet Mask
The subnet mask of the local interface.

Default Gateway
For AT-9400 Switches that support IPv4 routing, such as the AT-9424Ts and AT-9448Ts/XP switches, this field displays the IP address of the next hop of the switch's default route. The switch uses the default route when it receives a network packet for routing, but cannot find a route for it in the routing table. This field will contain 0.0.0.0 if no default route is defined on the switch.

For AT-9400 Switches that do not support IPv4 packet routing, such as the AT-9424T/GB and AT-9424T/SP switches, this field displays the default gateway address. This is the IP address of a router interface on your network. The switch's management software uses this address as the next hop to reaching a remote network device when the switch's local interface and the remote device are on different subnets. The default value is 0.0.0.0.

System Up Time
The length of time since the switch was last reset or power cycled.

The Software Information section displays the following information:

Application Software
The version number and build date of the AT-S63 Management Software.

Bootloader
The version number and build date of the AT-S63 bootloader.

The Hardware Information section displays the following information:

Power Information
The status of the main power supply, the redundant power supply (if present), and internal power consumption.

Temperature (Deg.C)
The ambient temperature as measured where the air enters the cooling vents on the side of the unit.

Fan Information
The speed or operating status of the system fan(s).

Chapter 2

Port Parameters

This chapter explains how to view and change the parameter settings of the ports on the switch. Examples of the parameters include port speed, duplex mode, and packet filtering.

This chapter contains the following procedures:

- ❒ “Configuring Port Parameters” on page 44
- ❒ “Displaying Port Parameters” on page 51
- ❒ “Displaying Port Statistics” on page 53
- ❒ “Resetting a Port to the Default Settings” on page 56

Configuring Port Parameters

To configure the parameter settings of a port on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 6.

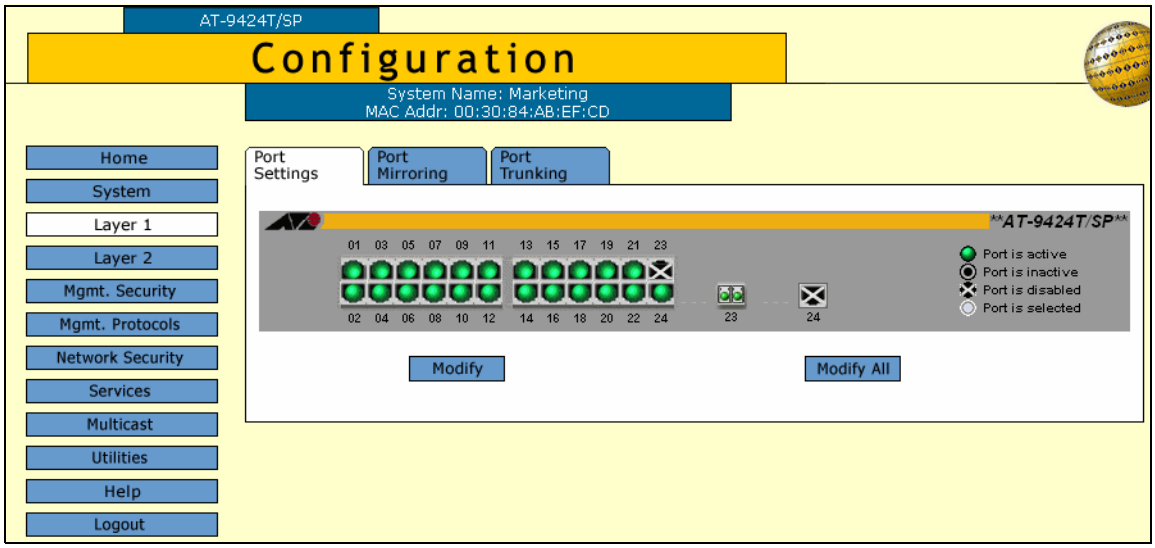

Figure 6. Port Settings Tab (Configuration)

   The Port Settings tab displays an image of the front of the switch. Ports with a valid link to an end node are green.

3. In the switch image, click a port to configure. The selected port turns white. You can configure more than one port at a time, though they must all be the same type (i.e., all twisted pair ports or all fiber optic ports). To deselect a port, click it again.

4. Click **Modify**. To configure all the ports, click **Modify All**.

The Port Configuration page is shown Figure 7.

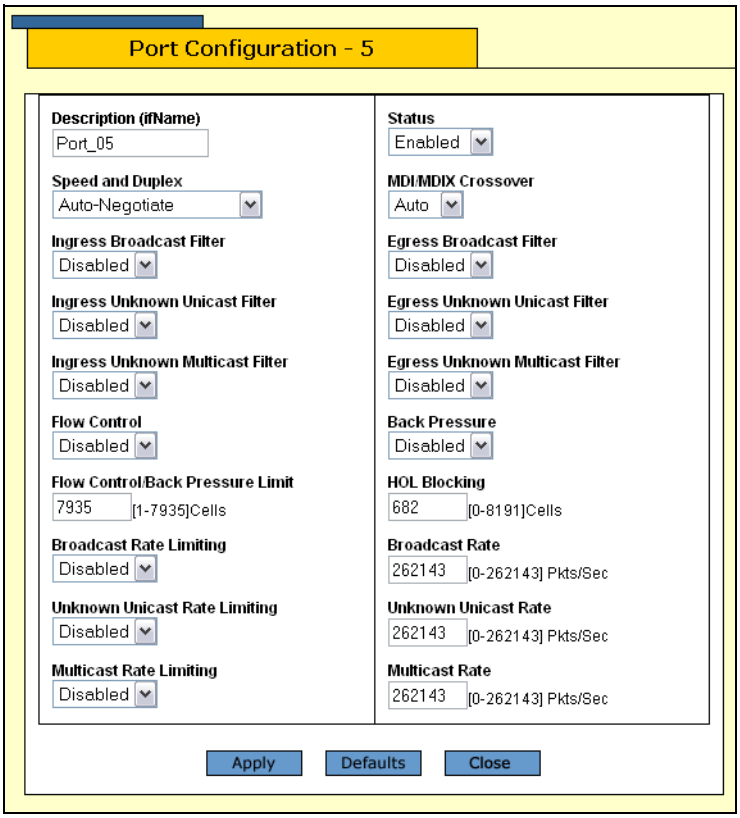

Figure 7. Port Configuration Page

Note
The Port Configuration page in the figure above is from a 10/100/1000 Mbps twisted pair port. The page for a fiber optic port will contain a subset of the parameters.

If you are configuring multiple ports and the ports have different settings, the Port Configuration page displays the settings of the lowest numbered port. After you have configured the settings of the port, all of its settings, including those that were not changed, are copied to the other selected ports.

The **Defaults** button at the bottom of the page returns the port settings to the default values, which can be found in Appendix A in the *AT-S63 Management Software Features Guide*.

5. Configure the following parameters as necessary.

Description (Name)
Use this selection to assign a name to a port, from 1 to 15 alphanumeric characters. Spaces are allowed, but do not use special characters, such as asterisks or exclamation points. (You cannot assign a name when you are configuring more than one port.)

Status
Use this selection to enable or disable a port. When disabled, a port does not accept or forward frames.

You might disable a port if a problem occurs with the end node or cable. After the problem has been fixed, you can enable the port again to resume normal operation.

You might also disable an unused port to secure it from unauthorized connections.

The possible settings are:

Enabled - The port forwards ingress and egress packets. This is the default setting.

Disabled - The port does not forward any ingress or egress packets.

Speed and Duplex
You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

If you select Auto-Negotiate for Auto-Negotiation, which is the default setting, the switch sets both speed and duplex mode for the port automatically.

Note the following about the operation of Auto-Negotiation on a switch port:

- In order for a switch port to successfully autonegotiate its duplex mode with an end node, the end node should also be using Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This results in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

  To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable Auto-Negotiation on the port and set its speed and duplex mode manually.

- If you disable Auto-Negotiation on a twisted pair port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. If you disable Auto-Negotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Possible settings are:

Auto-Negotiate: The port autonegotiates both speed and duplex mode. This is the default.

10Mbps - Half Duplex

10Mbps - Full Duplex

100Mbps - Half Duplex

100Mbps - Full Duplex

1Gb - Full Duplex (Applies only to 1000Base SFP and GBIC modules. This selection should not be used. An SFP or GBIC module should use Auto-Negotiation to set its speed and duplex mode.)

Note
A 10/100/1000Base-T twisted pair port must be set to Auto-Negotiation to operate at 1000 Mbps. You cannot manually configure a 10/100/1000Base-T twisted pair port to 1000 Mbps.

MDI/MDIX Crossover
The wiring configuration of a twisted pair port. This parameter does not apply to fiber optic ports. Possible settings are:

- Auto - Sets the port to automatically configure itself as MDI or MDIX, depending upon the end node. This is the default. This setting is only available when a port is set to Auto-Negotiation.
- MDI - Sets a port to MDI. This setting is only available when a port's speed and duplex mode are set manually.
- MDIX - Sets a port to MDIX. This setting is only available when a port's speed and duplex mode are set manually.

Ingress Broadcast Filter
Use this parameter to configure a port to forward or discard ingress broadcast packets. Possible settings are:

Enabled - The port discards ingress broadcast packets.

Disabled - The port forwards ingress broadcast packets. This is the default setting.

Egress Broadcast Filter
Use this parameter to configure a port to forward or discard egress broadcast packets. Possible settings are:

Enabled - The port discards egress broadcast packets.

Disabled - The port forwards egress broadcast packets. This is the default setting.

Ingress Unknown Unicast Filter
Use this parameter to configure a port to forward or discard unknown ingress unicast packets. The possible settings are:

Enabled - The port discards unknown ingress unicast packets.

Disabled - The port forwards unknown ingress unicast packets. This is the default setting.

Egress Unknown Unicast Filter
Use this parameter to configure a port to forward or discard unknown egress unicast packets. The possible settings are:

Enabled - The port discards unknown egress unicast packets.

Disabled - The port forwards unknown egress unicast packets. This is the default setting.

Ingress Unknown Multicast Filter
Use this parameter to configure a port to forward or discard unknown ingress multicast packets. Possible settings are:

Enabled - The port discards unknown ingress multicast packets.

Disabled - The port forwards unknown ingress multicast packets. This is the default setting.

Egress Unknown Multicast Filter
Use this parameter to configure a port to forward or discard unknown egress multicast packets. Possible settings are:

Enabled - The port discards unknown egress multicast packets.

Disabled - The port forwards unknown egress multicast packets. This is the default setting.

Flow Control
Sets flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses flow control to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time. Possible settings are:

Disabled - No flow control on the port. This is the default.

Enabled - Flow control is activated.

Back Pressure
Use this parameter to set backpressure on a port. This option only appears for ports operating in half-duplex mode. A port uses backpressure to control the flow of ingress packets. Possible settings are:

Enabled - Backpressure is enabled.

Disabled - Backpressure is disabled. This is the default.

Flow Control/Back Pressure Limit
Use this parameter to specify the threshold for flow control or backpressure. The threshold is specified in cells. A cell equals 128 bytes. The range is 1 to 7935. The default is 7935 cells.

HOL Blocking
HOL blocking sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port. The threshold is specified in number of cells. A cell is 128 bytes. The range is 1 to 8191. The default is 682.

Broadcast Rate Limiting
Use this parameter to enable or disable ingress broadcast packet limits. Possible settings are:

Enabled - Broadcast packet ingress rate limiting is enabled. To set the rate limit, use the Broadcast Rate parameter.

Disabled - Broadcast packet ingress rate limiting is disabled. This is the default.

Broadcast Rate
Use this parameter to set the broadcast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Unknown Unicast Rate Limiting
Use this parameter to enable or disable unknown ingress unicast packet limits. Possible settings are:

Enabled - Unknown unicast packet ingress rate limiting is enabled. To set the rate limit, use the Unknown Unicast Rate parameter.

Disabled - Unknown unicast packet ingress rate limiting is disabled. This is the default.

Unknown Unicast Rate
Use this parameter to set the unknown unicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Multicast Rate Limiting
Use this parameter to enable or disable ingress multicast packet limits. Possible settings are:

Enabled - Multicast packet ingress rate limiting is enabled. To set the rate limit, use the Multicast Rate parameter.

Disabled - Multicast packet ingress rate limiting is disabled. This is the default.

Multicast Rate
Use this parameter to set the multicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

6. After entering the desired changes, click **Apply**.

   The switch activates the parameter changes on the port.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying Port Parameters

To display the parameter settings of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 8.

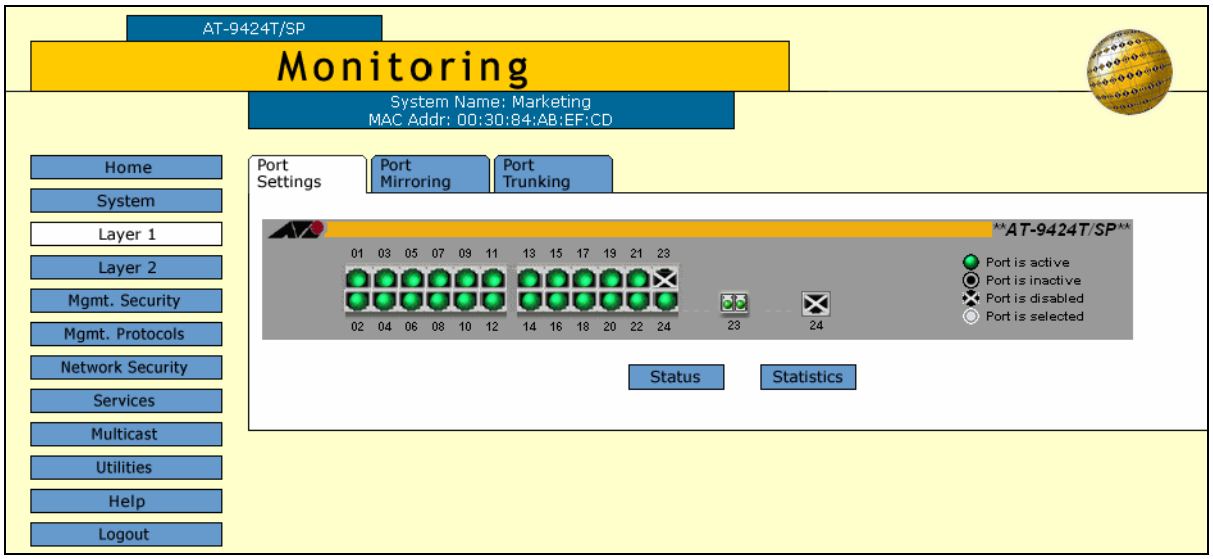

Figure 8. Port Settings Tab (Monitoring)

The Port Settings tab displays an image of the front of the switch. Ports with a valid link to an end node are green.

3. In the switch image, click a port. You can select more than one port. A selected port turns white. (To deselect a port, click it again.)
4. Click **Status**.

The Port Status page is shown in Figure 9.

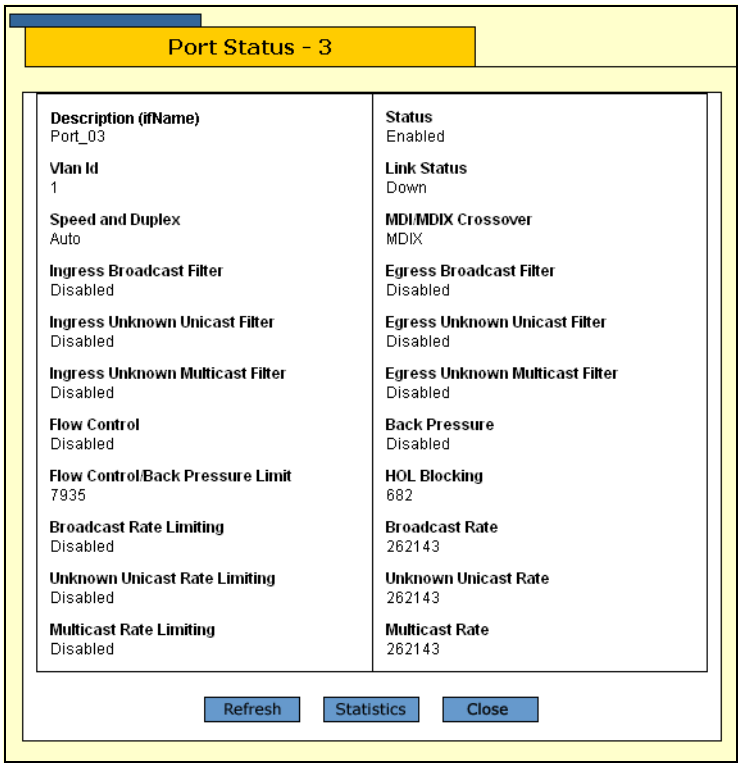

Figure 9. Port Status Page

For descriptions of the parameters, refer to “Configuring Port Parameters” on page 44.

Displaying Port Statistics

To display the statistics of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 8 on page 51. The Port Setting tab displays a image of the front of the switch. Ports with a valid link to an end node are green.
3. In the switch image, click a port. You can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
4. Click **Statistics**.

   The Port Statistics page is shown in Figure 10.

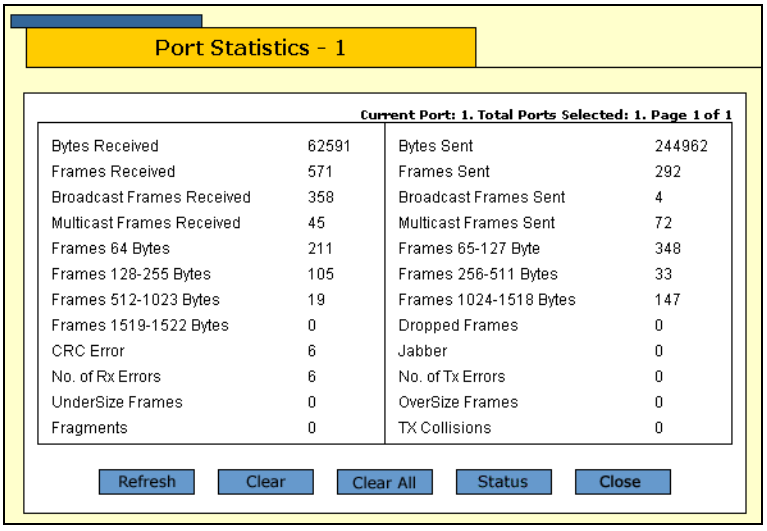

Figure 10. Port Statistics Page

The Port Statistics page displays a table with the following columns of information:

Bytes Received
Number of bytes received on the port.

Bytes Sent
Number of bytes transmitted from the port.

Frames Received
Number of frames received on the port.

Frames Sent
Number of frames transmitted from the port.

Broadcast Frames Received
Number of broadcast frames received on the port.

Broadcast Frames Sent
Number of broadcast frames transmitted from the port.

Multicast Frames Received
Number of multicast frames received on the port.

Multicast Frames Sent
Number of multicast frames transmitted from the port.

Frames 64 Bytes
Frames 65 - 127 Bytes
Frames 128 - 255 Bytes
Frames 256 - 511 Bytes
Frames 512 - 1023 Bytes
Frames 1024 - 1518 Bytes
Frames 1519 - 1522
Number of frames transmitted from the port, grouped by size.

CRC Error
Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Jabber
Number of occurrences of corrupted data or useless signals appearing on the port.

No. of Rx Errors
Total number of frames received on the port containing errors.

Undersize Frames
Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Frames
Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragments
Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received on the port.

TXCollisions
Number of transmit collisions.

5. To clear all the counters for the port, click **Clear**. To clear the counters for all ports on the switch, click **Clear All**. (The Clear and Clear All buttons are only available when you log on as a manager. They are not available when you log on as an operator.)

Resetting a Port to the Default Settings

To reset a port to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.

   The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 6 on page 44.
3. In the switch image, click a port to be returned to the default settings. The selected port turns white. You can reset more than one port at a time. (To deselect a port, click it again.)
4. Click **Modify**. To configure all of the ports, click **Modify All**.

   The Port Configuration page is displayed, as shown Figure 7 on page 45.
5. Click **Defaults**.

   The port(s) are returned to the default settings.

Chapter 3

Enhanced Stacking

This chapter contains the following procedures for setting up enhanced stacking:

- ❒ “Setting a Switch’s Enhanced Stacking Status” on page 58
- ❒ “Selecting a Switch in an Enhanced Stack” on page 60
- ❒ “Returning to the Master Switch” on page 62
- ❒ “Displaying the Enhanced Stacking Status” on page 63

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- Master - Starting a local or remote management session on a master switch of a stack allows you to easily transition to the other switches in the stack from the same management session.
- Slave - A slave switch can be remotely managed through a master switch or independently, such as through a local management session.
- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. It can also be managed remotely if it has a routing interface and the interface is designated as the local interface.

Note
The default setting for a switch is slave.

Note
The only switch whose stacking status can be changed through a web browser management session is the switch where you started the management session, typically a master switch. You cannot change the setting on a switch accessed through enhanced stacking. As an alternative, you can use a local management session or, if the switch has a local interface, you can use a Telnet or web browser management session.

To configure a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown in Figure 11.

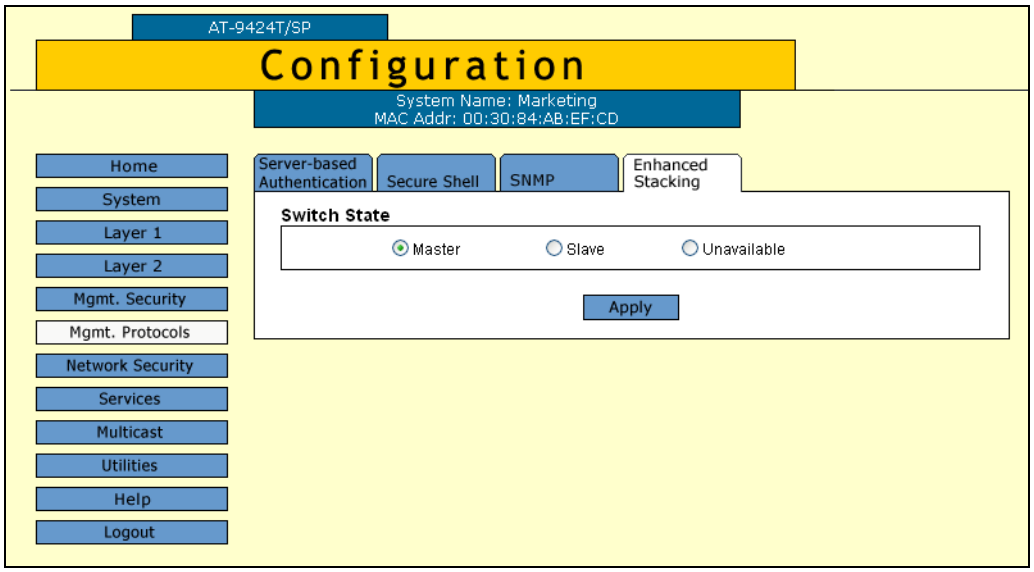

Figure 11. Enhanced Stacking Tab (Configuration)

4. Click the desired enhanced stacking status for the switch. The default is Slave.

5. Click **Apply**.

   The new setting for the enhanced stacking status is activated on the switch.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Selecting a Switch in an Enhanced Stack

This procedure explains how to select a switch to manage in an enhanced stack. You can manage only one switch at a time. When you start a web browser management session on an enhanced stack, you are initially managing the master switch where you started the session.

To select a switch in an enhanced stack to manage, perform the following procedure:

1. From the home page of the master switch, select **Enhanced Stacking**.

Note
If the Home page does not have an Enhanced Stacking menu option, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure:

To discover the switches in the stack, the master switch sends a broadcast packet out the ports of its local interface and monitors the interface for the responses from the switches. It displays the results in the Stacking Switches page. An example is shown in Figure 12.

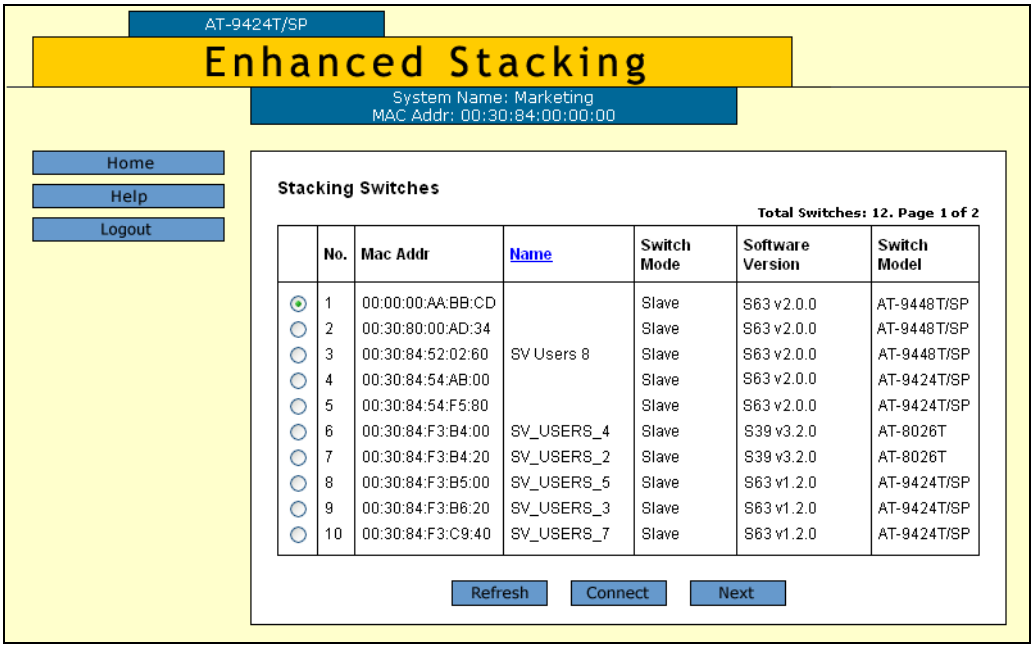
AT-9424T/SP
Enhanced Stacking
System Name: Marketing
MAC Addr: 00:30:84:00:00:00
Home
Help
Logout
Stacking Switches
Total Switches: 12. Page 1 of 2
No. Mac Addr Name Switch Mode Software Version Switch Model
1 00:00:00:AA:BB:CD Slave S63 v2.0.0 AT-9448T/SP
2 00:30:80:00:AD:34 Slave S63 v2.0.0 AT-9448T/SP
3 00:30:84:52:02:60 SV Users 8 Slave S63 v2.0.0 AT-9448T/SP
4 00:30:84:54:AB:00 Slave S63 v2.0.0 AT-9424T/SP
5 00:30:84:54:F5:80 Slave S63 v2.0.0 AT-9424T/SP
6 00:30:84:F3:B4:00 SV_USERS_4 Slave S39 v3.2.0 AT-8026T
7 00:30:84:F3:B4:20 SV_USERS_2 Slave S39 v3.2.0 AT-8026T
8 00:30:84:F3:B5:00 SV_USERS_5 Slave S63 v1.2.0 AT-9424T/SP
9 00:30:84:F3:B6:20 SV_USERS_3 Slave S63 v1.2.0 AT-9424T/SP
10 00:30:84:F3:C9:40 SV_USERS_7 Slave S63 v1.2.0 AT-9424T/SP
Refresh
Connect
Next

Figure 12. Stacking Switches Page

Note
The list does not include the master switch where you started the management session, nor any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

To refresh the list, click **Refresh**.

2. To start a management session on another switch in the enhanced stack, click the button to the left of the switch in the list. You can select only one switch.

   Note
   The web server mode (i.e., HTTP or HTTPS) must be the same on both the master switch and slave switch. For example, a master switch operating in the default HTTP mode can be used to manage switches configured for HTTP, but not HTTPS. For information on HTTPS, refer to the *AT-S63 Management Software Features Guide*.

3. Click **Connect**.

4. Enter a user name and password for the switch when prompted.

   The home page of the selected switch is displayed. You can now manage the selected switch.

Returning to the Master Switch

When you are finished managing the switch and want to manage another switch in the stack, select **Disconnect** from the main menu. This returns you to the Enhanced Stacking page (Figure 12 on page 60) of the master switch where you started the management session. At this point, you can do one of the following:

- Manage the master switch.
- Select another switch in the list to manage.
- Select **Logout** to end your management session.

Displaying the Enhanced Stacking Status

To display the enhanced stacking status of the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Protocols** option.
3. Select the **Enhanced Stacking** tab.

   The Enhanced Stacking tab is shown Figure 13.

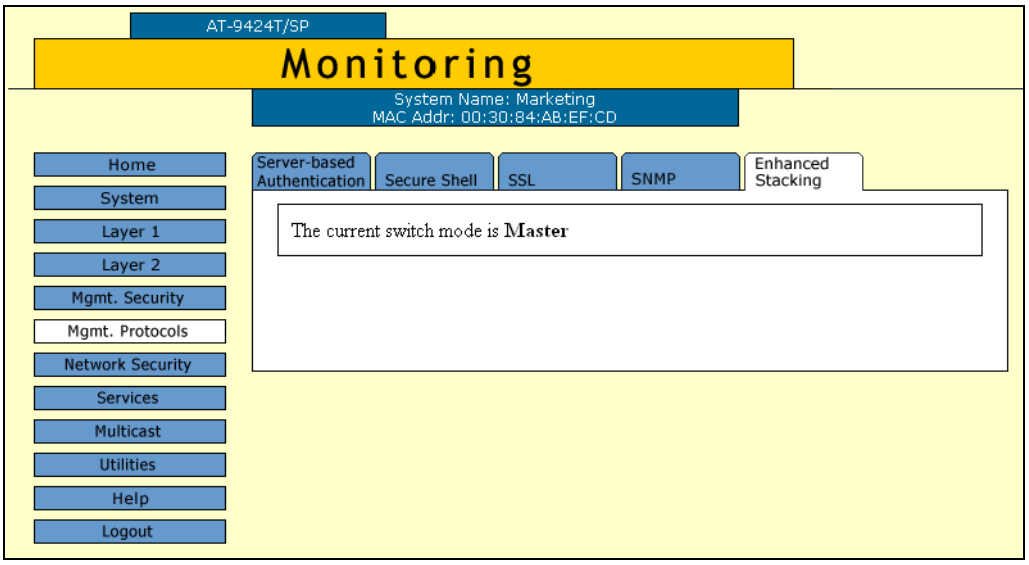

Figure 13. Enhanced Stacking Tab (Monitoring)

The information in the tab states the current enhanced stacking status of the switch as master, slave, or unavailable.

Chapter 4

SNMPv1 and SNMPv2c

This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

- ❒ “Enabling or Disabling SNMP Management” on page 66
- ❒ “Creating a New SNMPv1 and SNMPv2c Community” on page 68
- ❒ “Modifying an SNMPv1 and SNMPv2c Community” on page 71
- ❒ “Deleting an SNMPv1 and SNMPv2c Community” on page 72
- ❒ “Displaying the SNMPv1 and SNMPv2c Communities” on page 73

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14.

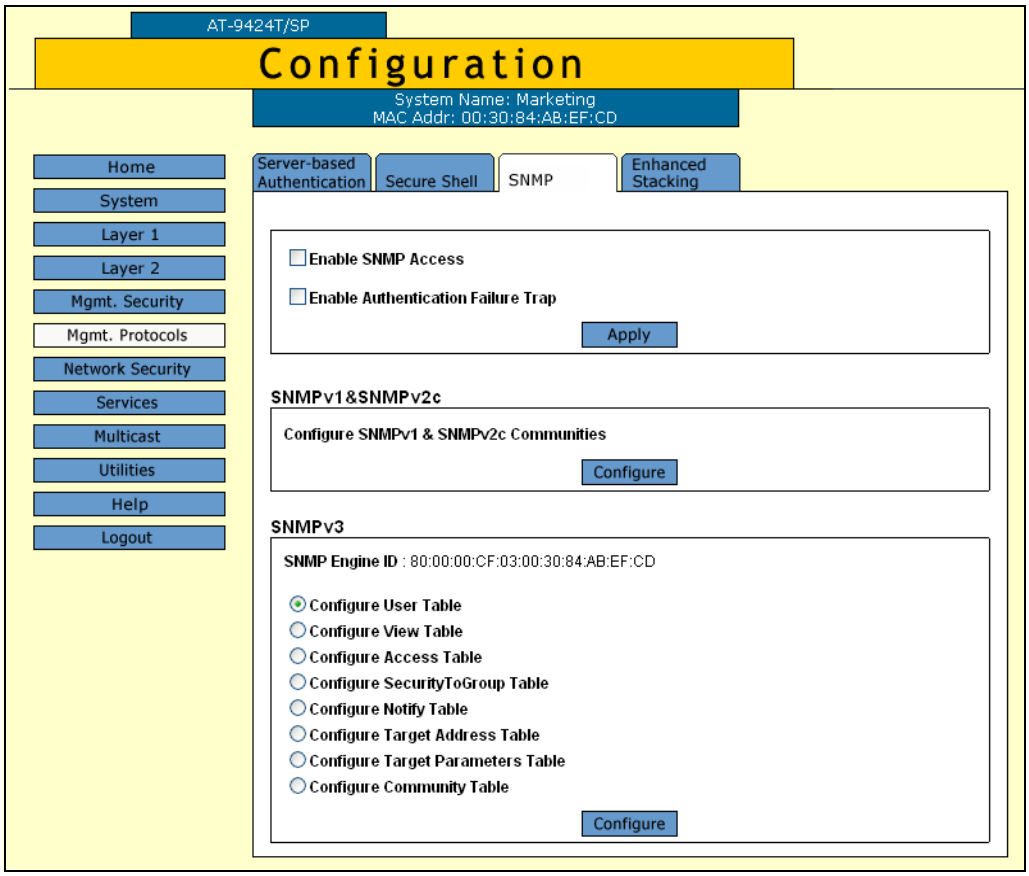

Figure 14. SNMP Tab (Configuration)

4. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates the feature is enabled, meaning the switch can be managed from an SNMP management station. No check indicates the feature is disabled. The default is disabled.

5. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates the switch sends the trap.

6. Click **Apply**.

   A change to SNMP access is immediately activated on the switch.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Creating a New SNMPv1 and SNMPv2c Community

To create a new SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 66.
4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15.

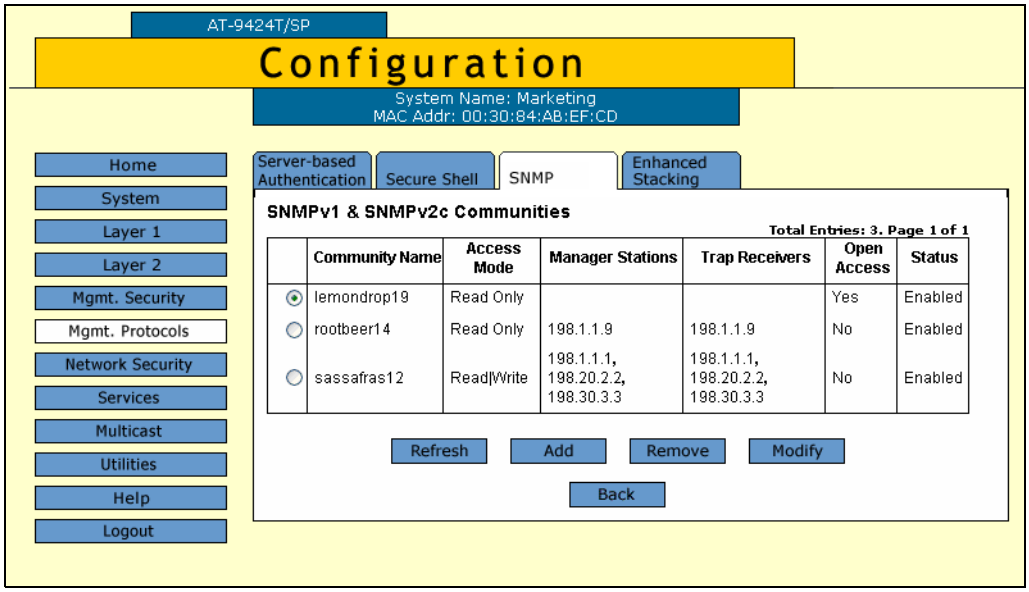

Figure 15. SNMPv1 & SNMPv2c Communities Tab

The table in the tab displays the existing community strings. The columns of the table are defined here:

Community Name
The name of a community string.

Access Mode
The access mode of a community string. A string with a Read Only access mode permits the viewing of the MIB objects on the switch. A string with a Read/Write access mode permits both viewing and changing the SNMP MIB objects.

Manager Stations
The IP addresses of management workstations permitted to use a string with a closed access status.

Trap Receivers
The IP addresses of trap receivers to receive traps from the switch.

Open Status
The access status of a community string. Yes means the string has an open status and that any management workstation can use it. No means the string has a closed status and that only those workstations whose IP addresses are assigned to the string are permitted to use it.

Status
The operating status of a community string. Enabled means the string is available for use and Disabled means it is unavailable.

5. To create a new community string, click **Add**. The Add New SNMPv1 & SNMPv2c Community page is shown in Figure 16 on page 69.

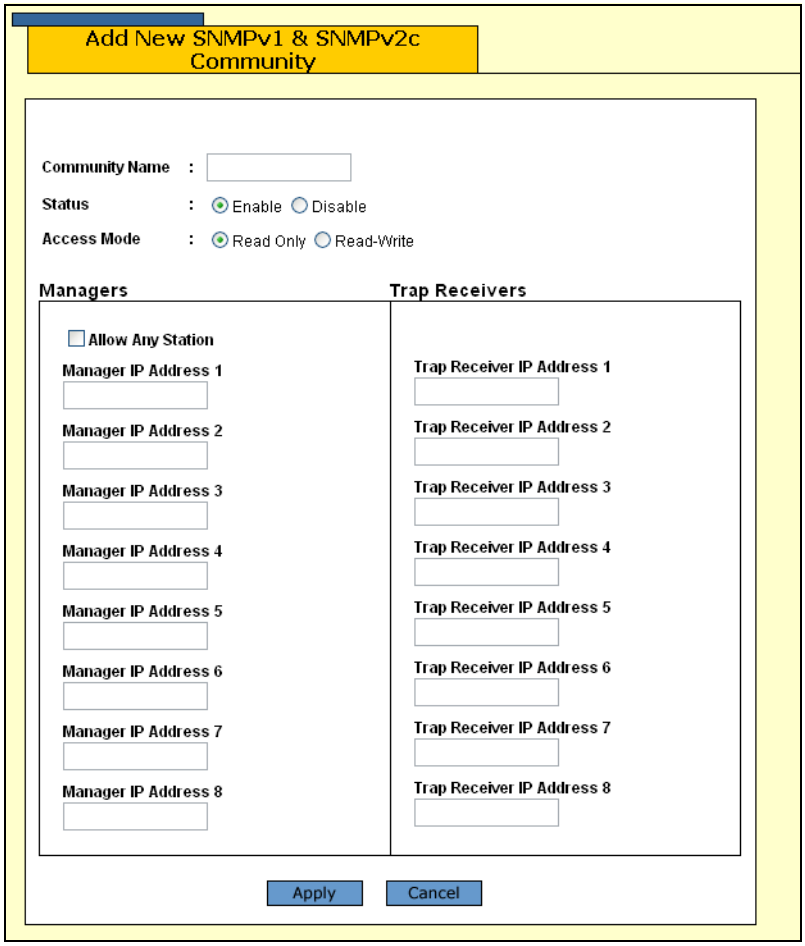
Add New SNMPv1 & SNMPv2c Community
Community Name :
Status : Enable Disable
Access Mode : Read Only Read-Write
Managers
Trap Receivers
Allow Any Station
Manager IP Address 1
Manager IP Address 2
Manager IP Address 3
Manager IP Address 4
Manager IP Address 5
Manager IP Address 6
Manager IP Address 7
Manager IP Address 8
Trap Receiver IP Address 1
Trap Receiver IP Address 2
Trap Receiver IP Address 3
Trap Receiver IP Address 4
Trap Receiver IP Address 5
Trap Receiver IP Address 6
Trap Receiver IP Address 7
Trap Receiver IP Address 8
Apply
Cancel

Figure 16. Add New SNMPv1 & SNMPv2c Community Page

6. Configure the following parameters:

   Community Name
   Enter the new community string. The name can be up to 32 alphanumeric characters. No spaces or special characters (such as /, #, or &) are allowed.

   Status
   Enable or disable the community string. A disabled community string cannot be used to access the switch. The default is enabled.

   Access Mode
   Specify the access mode for the SNMP community string. A string with a Read Only access mode can only be used to view the MIB objects on the switch. A string with a Read/Write access mode can be used to both view and change the SNMP MIB objects.

   Allow Any Station
   Set the community string as opened or closed. If there is no check in the box next to the option, the community string is closed; only those workstations whose IP addresses are assigned to the community string can use it. If there is a check in the box, the string is open, meaning any SNMP management workstation can use it to access the switch.

   Manager IP Address 1 through **Manager IP Address 8**
   Specify the IP addresses of management workstations. If you gave the community string a closed status, use these fields to specify the IP addresses of up to eight management workstations permitted to use the community string to access the switch. Entering manager IP addresses for a community string with an open status has no affect on the string.

   Trap Receiver IP Address 1 through **Trap Receiver IP Address 8**
   Specify the IP addresses of up to eight trap receivers. These are nodes on your network, such as your management workstation, to act as trap receivers for the switch.

7. Click **Apply**.

   The new community string is now available on the switch.

8. Repeat this procedure starting with step 4 to add more community strings.

9. To permanently save your changes, select the **Save Config** menu option.

Modifying an SNMPv1 and SNMPv2c Community

To modify an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 66.
4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15 on page 68.
5. Click the button next to the community name to be modified and click **Modify**. You can modify only one community string at a time.

   The settings of the selected SNMP community string are displayed in the Modify SNMPv1 & SNMPv2c Community page.
6. Modify the parameters as needed. For parameter definitions, refer to "Creating a New SNMPv1 and SNMPv2c Community" on page 68. You cannot change the community name of a string.
7. Click **Apply**.

   The modifications are activated on the community string.
8. To permanently save the changes, select the **Save Config** menu option.

Deleting an SNMPv1 and SNMPv2c Community

To delete an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 14 on page 66.
4. In the SNMPv1 & SNMPv2c section, click **Configure**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 15 on page 68.
5. Click the button next to the community name to delete and click **Remove**. You can delete only one community string at a time.

   A warning message is displayed.
6. Click **OK**.

   The community string is deleted from the switch.
7. To permanently save the change, select the **Save Config** menu option.

Displaying the SNMPv1 and SNMPv2c Communities

To display the SNMPv1 and SNMPv2c communities, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Protocols** option.
3. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 17.

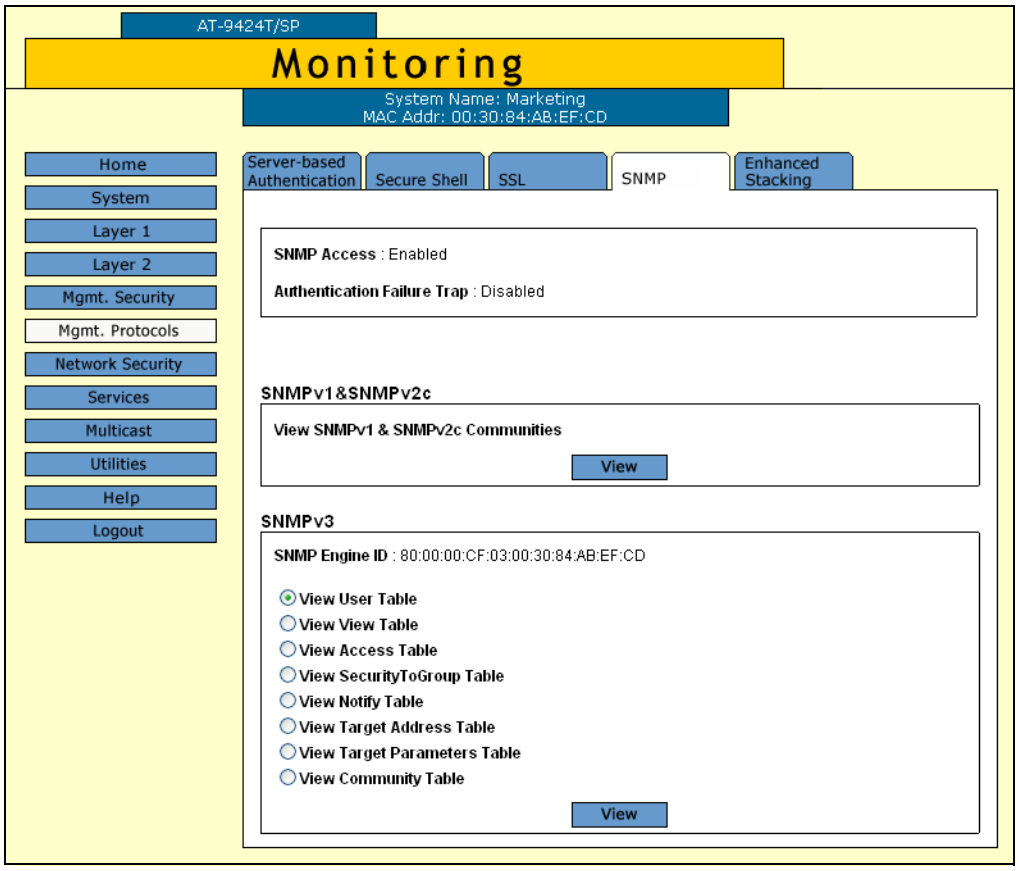

Figure 17. SNMP Tab (Monitoring)

4. In the SNMPv1 & SNMPv2c section, click **View**.

   The SNMPv1 & SNMPv2c Communities tab is shown in Figure 18.

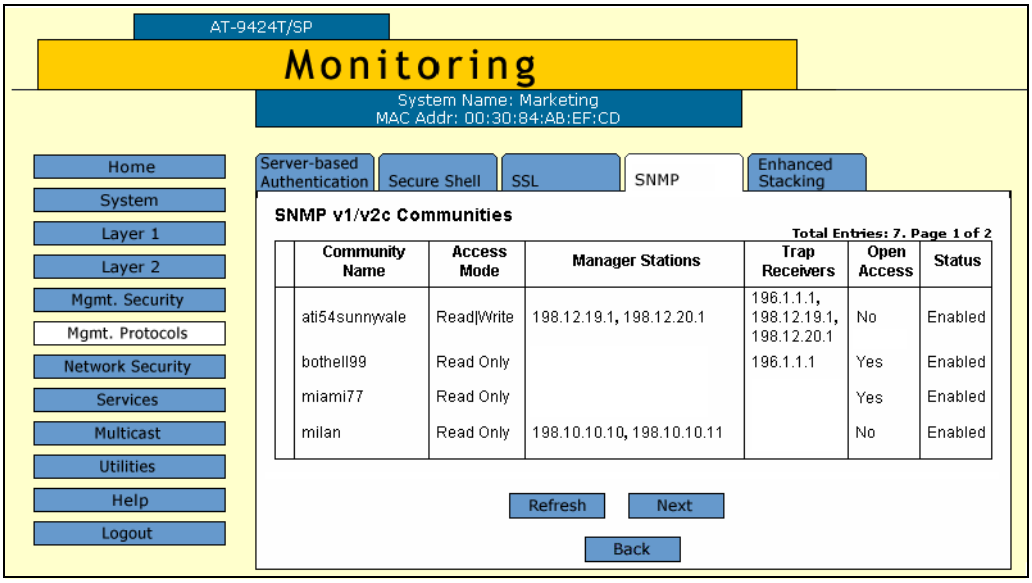

Figure 18. SNMPv1 & SNMPv2c Communities Tab (Monitoring)

The columns in the table are defined here:

Community Name
The name of a community string.

Access Mode
The access mode of a community string. A string with a Read Only access mode permits the viewing of the MIB objects on the switch. A string with a Read/Write access mode permits both viewing and changing the SNMP MIB objects.

Manager Stations
The IP addresses of management workstations permitted to use a string with a closed access status.

Trap Receivers
The IP addresses of trap receivers to receive traps from the switch.

Open Status
The access status of a community string. Yes means the string has an open status and any management workstation can use it. No means the string has a closed status and that those workstations whose IP addresses are assigned to the string are permitted to use it.

Status
The operating status of a community string. Enabled means the string is available for use and Disabled means it is unavailable.

Chapter 5

MAC Address Table

This chapter contains instructions on how to view the MAC addresses in the MAC address table. It also explained how to add static addresses to the table. This chapter contains the following procedures:

- ❒ “Displaying the MAC Address Table” on page 76
- ❒ “Adding Static Unicast and Multicast MAC Addresses” on page 79
- ❒ “Deleting Unicast and Multicast MAC Addresses” on page 81
- ❒ “Deleting All Dynamic MAC Addresses” on page 82
- ❒ “Changing the Aging Time” on page 83

Displaying the MAC Address Table

To view the MAC address table, perform the following procedure:

1. From the Home page, select **Monitoring** or **Configuration**.
2. From the Monitoring or Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 19.

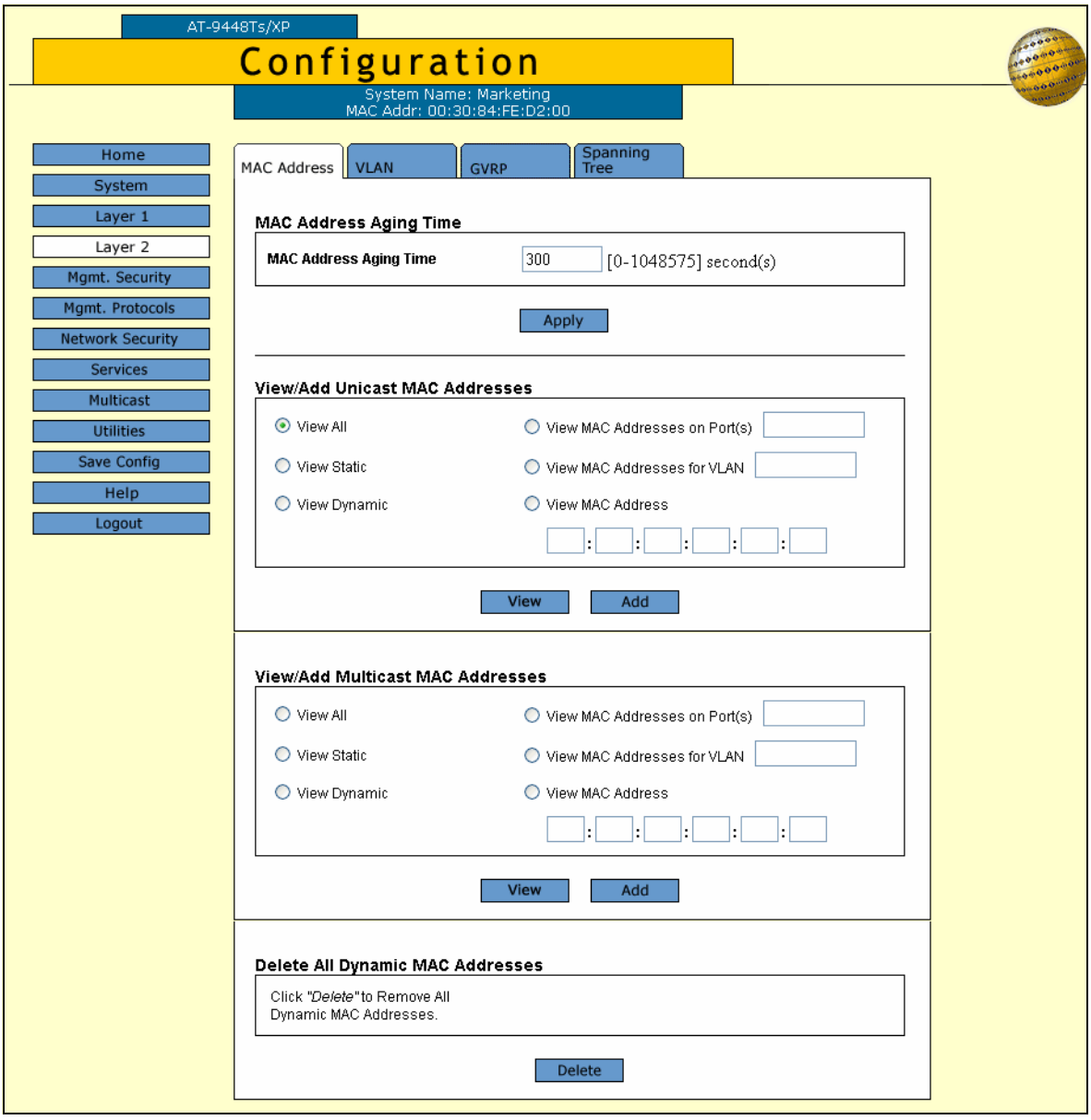

Figure 19. MAC Address Tab (Configuration)

The View Unicast MAC Addresses section and the View Multicast MAC Addresses section display unicast and multicast addresses, respectively. The options function the same in both sections. You can select only one option at a time.

View All
Displays all dynamic and static unicast or multicast addresses in the MAC address table.

View Static
Displays just the static unicast or multicast addresses assigned to the ports.

View Dynamic
Displays just the dynamic addresses learned on the ports.

View MAC Addresses on Port
Displays the dynamic and static MAC addresses of a particular port. You can specify more than one port at a time.

View MAC Addresses for VLAN
Displays the static and dynamic addresses learned on the tagged and untagged ports of a VLAN. You specify the VLAN by entering the VLAN ID number. You can specify only one VLAN at a time.

View MAC Address
Displays the port number where a MAC address was assigned or learned. In some situations, you might want to know which port learned a particular MAC address. You could display the MAC address table and scroll through the list looking for the MAC address, but if the switch is part of a large network, finding the address could prove difficult. This option allows you to specify the MAC address and let the AT-S63 Management Software automatically locate the port where the address was learned.

3. After selecting an option, click **View.**

Figure 20 shows an example of viewing all unicast MAC addresses.

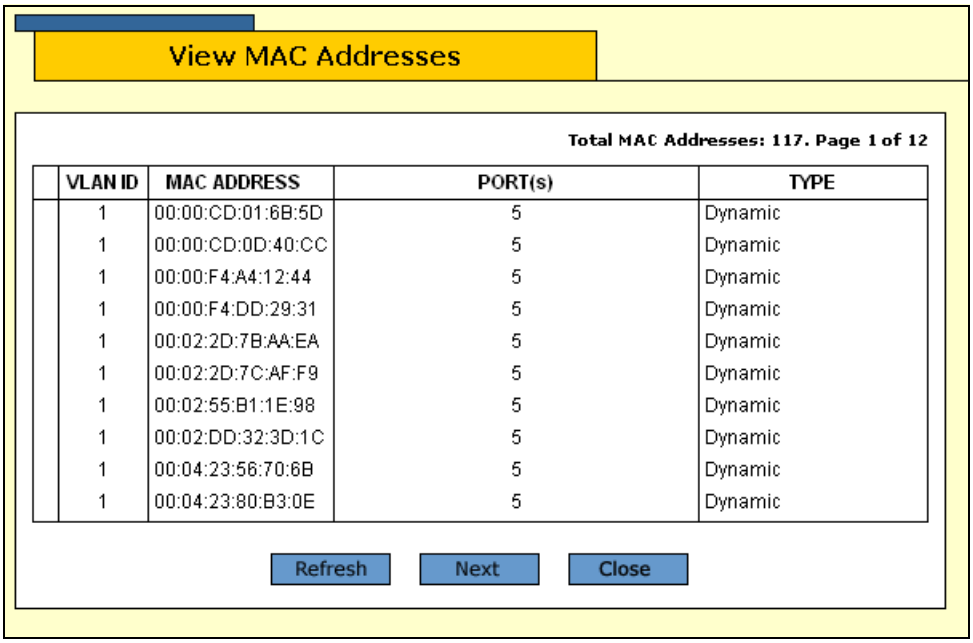

Figure 20. View MAC Addresses Page

The View MAC Addresses page displays a table that contains the following columns of information:

VLAN ID
The ID number of the VLAN where the port is a member.

MAC Address
The static or dynamic MAC address.

Port(s)
The port where the address was learned or assigned. The MAC address with port “CPU” is the address of the switch.

Type
The type of the address: static or dynamic.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to a port. A switch port can have up to 255 static MAC addresses.

To add a static address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 19 on page 76.
3. To add a static unicast address, click **Add** in the View/Add Unicast MAC Addresses section. To add a static multicast address, click **Add** in the View/Add Multicast MAC Addresses section.

   The Add MAC Address page is shown in Figure 21.

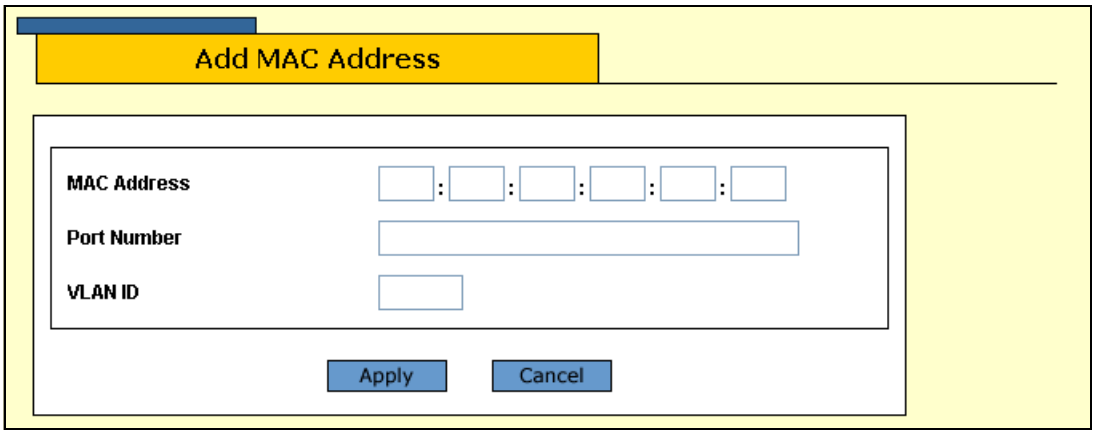

Figure 21. Add MAC Address Page

4. Configure the following parameters as necessary.

   MAC Address
   Specifies the new static unicast or multicast MAC address.

   Port Number
   Specifies the number of the port on the switch where the static address is to be assigned. For a static unicast address, you can enter only one port.

   For a static multicast address, you must specify the port when the multicast application is located as well as the ports where the host nodes are connected. Assigning the address only to the port where the

multicast application is located results in the failure of the multicast packets to be properly forwarded to the host nodes. You can specify the ports individually (e.g., 1,4,5), as a range (e.g., 11-14) or both (e.g., 15-17,22,24).

VLAN ID
Specifies the VLAN ID where the port is a member.

5. Click **Apply**.
6. Repeat this procedure to add other static addresses to the switch.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting Unicast and Multicast MAC Addresses

To delete a static or dynamic unicast or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 19 on page 76.
3. Display the MAC addresses on the switch by selecting one of the options. For instructions, refer to "Displaying the MAC Address Table" on page 76.
4. Click the button next to the MAC address to be deleted from the switch. You can only delete one address at a time.

   Note
   You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

5. Click **Remove**.

   The MAC address is deleted from the table.
6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting All Dynamic MAC Addresses

To delete all dynamic unicast and multicast MAC addresses from the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 19 on page 76.
3. In the Delete All Dynamic MAC Addresses section, click **Delete**.

   All dynamic unicast and multicast MAC address are deleted from the switch. The switch immediately begins to learn new dynamic addresses.

Changing the Aging Time

This procedure changes the aging time of the MAC address table. The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. The switch deletes an address from the table if no packets are sent to or received from the address for the period of time specified in the timer. This prevents the table from becoming full of addresses of inactive nodes. The default setting for the aging time is 300 seconds (5 minutes).

To configure the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.

   The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 19 on page 76.
3. In the MAC Address Aging Time field, enter a new value in seconds. The range is 0 to 1048575 seconds. The default is 300 seconds (5 minutes). The value 0 disables the aging timer. If the aging timer is disabled, inactive dynamic addresses are not deleted from the table and the switch stops learning new addresses after the table reaches maximum capacity.
4. Click **Apply**.

   The new MAC address aging time is activated on the switch.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Chapter 6

Static Port Trunks

This chapter contains the procedure for managing static port trunks. The sections in this chapter are:

- ❒ “Creating a Static Port Trunk” on page 86
- ❒ “Modifying a Static Port Trunk” on page 90
- ❒ “Deleting a Port Trunk” on page 92
- ❒ “Displaying the Port Trunks” on page 93

Note
LACP trunks are not supported from the web browser interface.

Creating a Static Port Trunk

Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the remote device. Connecting the cables prior to configuring the trunk can create a loop in your network topology. This can cause a broadcast storm and poor network performance.

Note

Prior to creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port that will be a part of the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S63 Management Software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

To create a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 22.

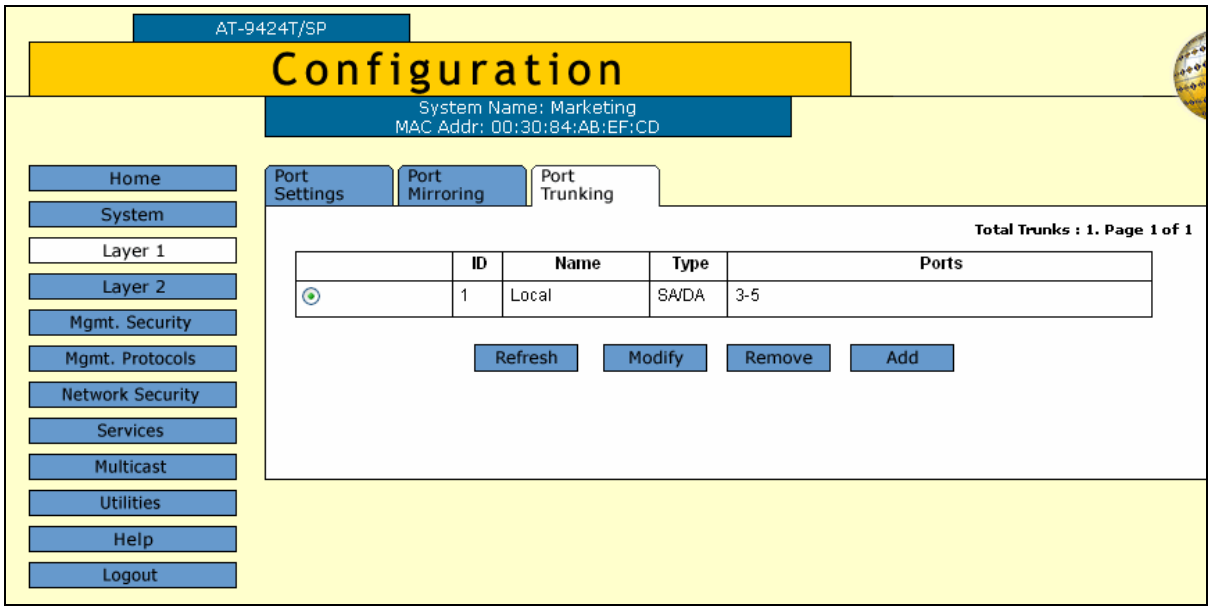

Figure 22. Port Trunking Tab (Configuration)

The tab displays the current static trunks in a table with the following columns of information:

ID
The ID number of the trunk.

Name
The name of the trunk.

Type
The load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

Ports
The ports of the trunk.

4. To create a new static trunk, click **Add**.

   The Add New Trunk page is shown in Figure 23.

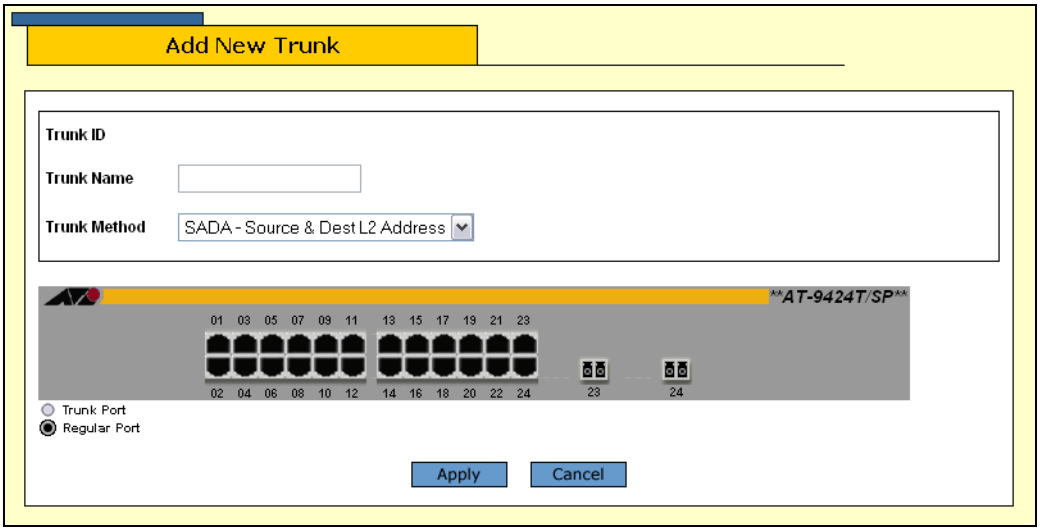

Figure 23. Add New Trunk Page

5. Click the Trunk Name field and enter a name for the static trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

6. From the Trunk Method pull-down menu, select a load distribution method for the trunk. The possible settings are:

   SA - Source MAC address (Layer 2)

   DA - Destination MAC address (Layer 2)

   SA/DA - Source MAC address /destination MAC address (Layer 2)

   SI - Source IP address (Layer 3)

   DI - Destination IP address (Layer 3)

   SI/DI - Source IP address /destination IP address (Layer 3)

7. In the switch image, click the ports to be in the port trunk. A selected port changes to white. An unselected port is black. A static port trunk can contain up to eight ports.

Note
Allied Telesis does not recommend using paired twisted pair ports with GBIC or SFP slots in a port trunk. The operation of a port trunk may be unpredictable if a paired port were to transition to the redundant uplink status mode.

8. Click **Apply**.

   The new port trunk is now active on the switch.

9. To permanently save your changes, select the **Save Config** option in the Configuration menu.

10. Configure the ports on the remote device for port trunking.

11. Connect the cables to the ports of the trunk on the switch and on the remote device.

    The port trunk is ready for network operations.

Modifying a Static Port Trunk

This section contains the procedure for modifying a static port trunk on the switch. You can change the name and ports of a trunk from the web browser interface, but not the load distribute method. Be sure to review the guidelines in the *AT-S63 Management Software Features Guide* before performing the procedure:

> **Caution**
> Disconnect all data cables from the ports of the trunk on the switch before performing this procedure if you plan to add or remove ports from the trunk. Leaving the cables connected can form a loop in your network topology. This can cause a broadcast storm and poor network performance.

Note the following before performing this procedure:

- If you are adding a port and the port will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you should check to see if its settings are appropriate prior to adding it.
- If you are adding a port and the port will not be the lowest numbered port in the trunk, its settings are automatically changed to match the settings of the existing ports in the trunk.
- If you are adding a port to a trunk, check to be sure that the new port is an untagged member of the same VLAN as the other trunk ports. A trunk cannot contain ports that are untagged members of different VLANs.
- You cannot change the load distribution method of a static port trunk from the web browser manager interface, but you can from the menus and command line interfaces.

To modify a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 22 on page 87.
4. Click the button next to the port trunk to be modified and click **Modify**.

The Modify Trunk page is shown in Figure 24.

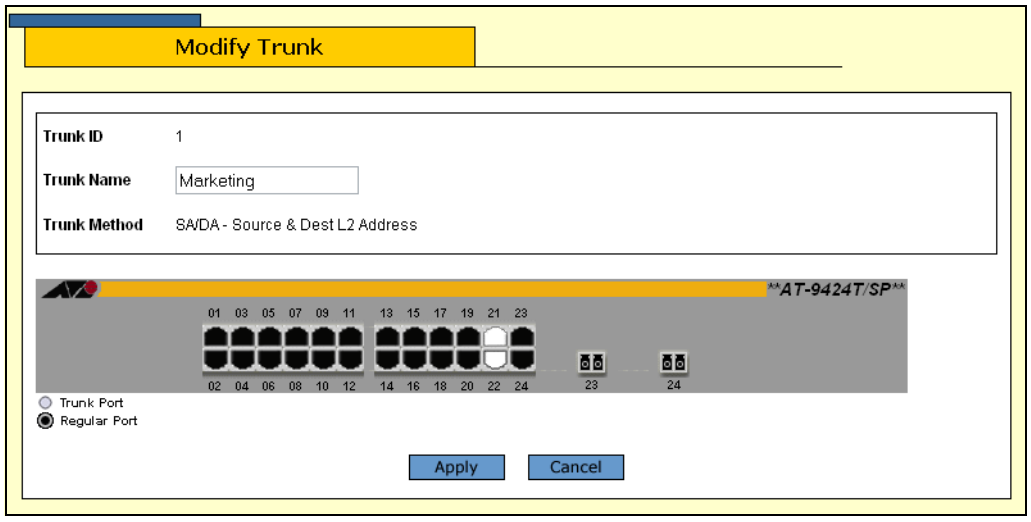

Figure 24. Modify Trunk Page

5. To change the name of the trunk, click the Trunk Name field and enter the new name. The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

6. To add or remove ports from a trunk, click the ports in the graphical image of the switch. A selected port changes to white. An unselected port is black. A static port trunk can contain up to eight ports.

7. Click **Apply**. Changes to a port trunk are activated on the switch.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

9. Reconnect the cables to the ports of the trunk.

Deleting a Port Trunk

Caution
Disconnect the cables from the port trunk on the switch before performing this procedure. Deleting the trunk without first disconnecting the cables can result in the formation of a loop in your network topology. This can cause a broadcast storm and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 22 on page 87.
4. Click the button next to the port trunk to be deleted and click **Remove**. You can delete only one trunk at a time.

   The port trunk is deleted from the switch.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Port Trunks

To display the port trunks, perform the following procedure:

1. From the home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.
3. Select the **Port Trunking** tab.

   The Port Trunking tab is shown in Figure 25.

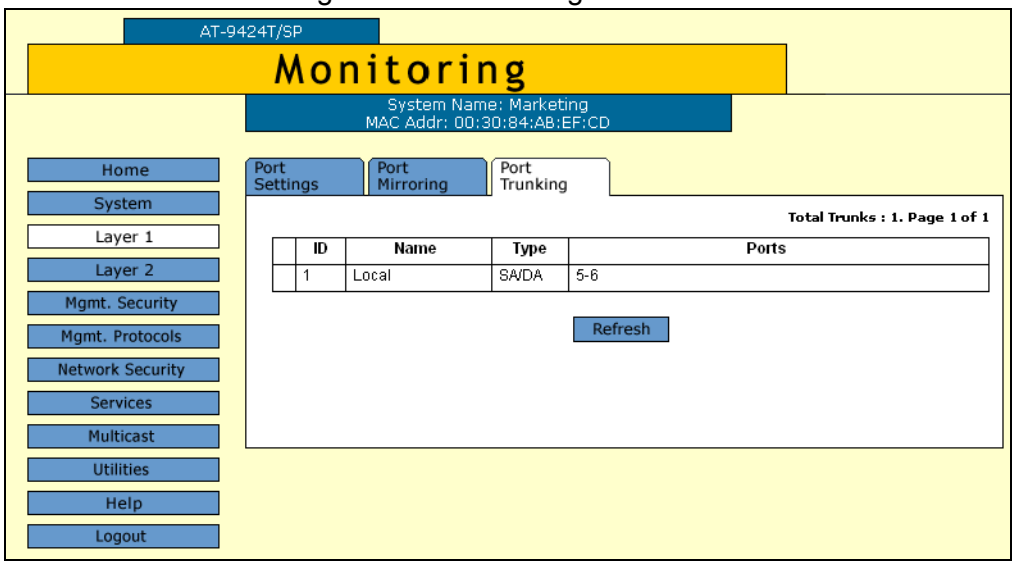

Figure 25. Port Trunking Tab (Monitoring)

The Port Trunking tab displays a table with the following columns of information:

ID
The ID number of the trunk.

Name
The name of the trunk.

Type
The load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

Ports
The ports of the trunk.

Chapter 7

Port Mirroring

This chapter contains the procedures for managing the port mirroring feature. The sections in the chapter include:

- ❒ “Creating a Port Mirror” on page 96
- ❒ “Modifying a Port Mirror” on page 99
- ❒ “Disabling a Port Mirror” on page 100
- ❒ “Deleting a Port Mirror” on page 101
- ❒ “Displaying the Port Mirror” on page 102

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 26.

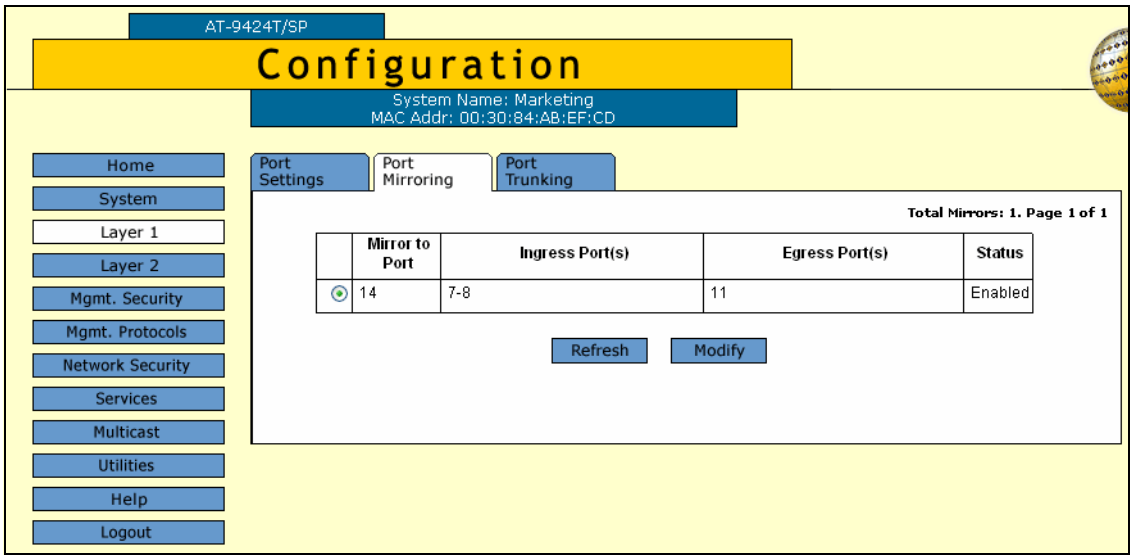

Figure 26. Port Mirroring Tab (Configuration)

The tab displays a table with the following columns:

Mirror to Port
Specifies the destination port of the mirrored traffic. There can be only one destination port. If this column contains a 0 (zero), there is no port mirror.

Ingress Ports
Specifies the ports whose ingress traffic is to be mirrored to the destination port.

Egress Ports
Specifies the ports whose egress traffic is to be mirrored to the destination port.

Status
Specifies the status of the port mirror as either enabled or disabled.

4. Click **Modify**.

   The Modify Mirror page is shown in Figure 27.

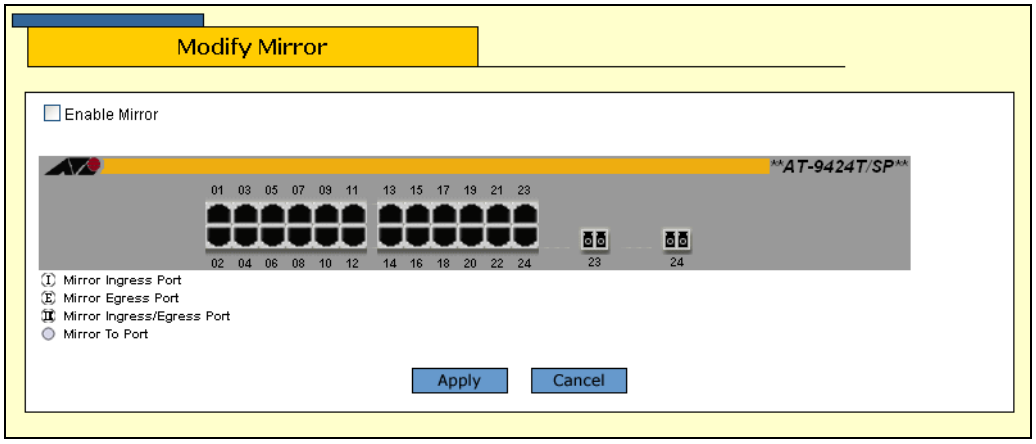

Figure 27. Modify Mirror Page

5. Click the ports to be in the port mirror. Clicking a port toggles it through the following possible settings:

   The destination (mirror) port. There can be only one destination port.

   A source port. The port's ingress traffic is mirrored to the destination port.

   A source port. The port's egress traffic is mirrored to the destination port.

   A source port. The port's ingress and egress traffic is mirrored to the destination port.

   Not part of a port mirror.

   You can mirror one port, a few ports, or all of the ports on the switch, with the exception, of course, of the destination port.

   Note
   To create a mirror port for the Denial of Service defenses, specify only the destination port. The management software automatically determines the source ports.

Figure 28 shows an example of the Modify Mirror page configured for a port mirror. The ingress and egress traffic on ports 1, 2, and 7 to 10 is being mirrored to the destination port 11.

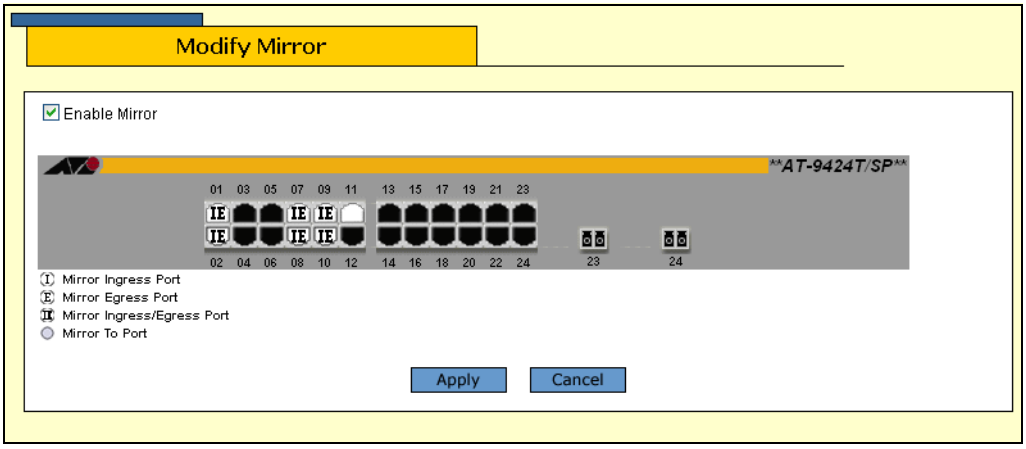

Figure 28. Example of a Modify Mirror Page

6. After selecting the destination and source ports, click the **Enable Mirror** check box.

7. Click **Apply**.

   The port mirror is now active on the switch. You can connect a data analyzer to the destination port to monitor the traffic on the source ports.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Port Mirror

To modify a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 26 on page 96.
4. Click **Modify**.

   The Modify Mirror page is shown in Figure 27 on page 97.
5. Change the ports of the port mirror, as needed. Clicking a port toggles it through the possible settings, which are as follows:

   The destination (mirror) port. There can be only one destination port. To change the destination port, you must first change the current destination port to one of the other settings.

   A source port. The port's ingress traffic is mirrored to the destination port.

   A source port. The port's egress traffic is mirrored to the destination port.

   A source port. The port's ingress and egress traffic is mirrored to the destination port.

   Not part of a port mirror.
6. Click **Apply**.

   The changes to the port mirror are now active on the switch.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Disabling a Port Mirror

This procedure disables a port mirror. When disabled, a port mirror stops copying traffic from the source ports to the destination port. However, the destination port is still reserved for port mirroring. To delete the port mirror so that the destination port can be used for normal network operations, refer to “Deleting a Port Mirror” on page 101.

To disable a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 26 on page 96.
4. Click **Modify**.

   The Modify Mirror page is shown in Figure 27 on page 97.
5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.
6. Click **Apply**.

   The port mirror is now disabled. The switch stops copying the traffic on the source ports to the destination port.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Port Mirror

To delete a port mirror so that you can use the destination port for normal network operations, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 26 on page 96.
4. Click **Modify**.

   The Modify Mirror page is shown in Figure 27 on page 97.
5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.
6. Click the destination port (white port) until it is black.
7. Click **Apply**.

   The destination port can now be used for normal network operations.
8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Port Mirror

To display the port mirror, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 1** option.
3. Select the **Port Mirroring** tab.

   The Port Mirroring tab is shown in Figure 29.

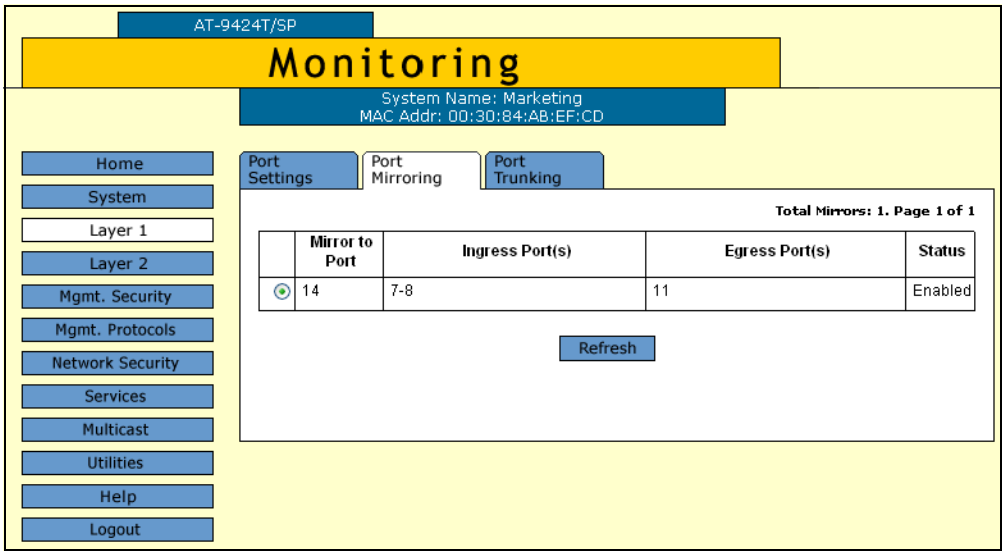

Figure 29. Port Mirroring Tab (Monitoring)

The tab displays a table with the following columns:

Mirror to Port
The destination port where the traffic is copied and where the network analyzer is located.

Ingress Port(s)
The source ports whose ingress traffic is mirrored to the destination port.

Egress Port(s)
The source ports whose egress traffic is mirrored to the destination port.

Status
The status of the mirroring feature. The possible settings are:

Enabled - Traffic is being copied to the destination port.

Disabled - No traffic is being mirrored.

Section II

Advanced Operations

This section has the following chapters:

- Chapter 8, “File System” on page 105
- Chapter 9, “File Downloads and Uploads” on page 111
- Chapter 10, “Event Logs and Syslog Client” on page 119
- Chapter 11, “Classifiers” on page 135
- Chapter 12, “Access Control Lists” on page 147
- Chapter 13, “Class of Service” on page 155
- Chapter 14, “Quality of Service” on page 165
- Chapter 15, “Denial of Service Defenses” on page 187
- Chapter 16, “IGMP Snooping” on page 193

Chapter 8
File System

This chapter contains the procedures for working with the switch's file system. The sections include:

- ❒ "Listing the Files in Flash Memory or on a Compact Flash Card" on page 106
- ❒ "Selecting an Active Boot Configuration File" on page 109

Listing the Files in Flash Memory or on a Compact Flash Card

This procedure displays the files stored in the switch's flash memory or on a compact flash card. (Not all AT-9400 Switches support a flash card slot.)

> **Note**
> You cannot copy, rename, or delete files from a web browser management session. Those tasks can be performed from the menus and command line interfaces.

To display a list of the system files stored in the switch's flash memory or on a compact flash card, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Utilities** option.
3. Select the **File System** tab.

   The FIle System tab is shown in Figure 30.

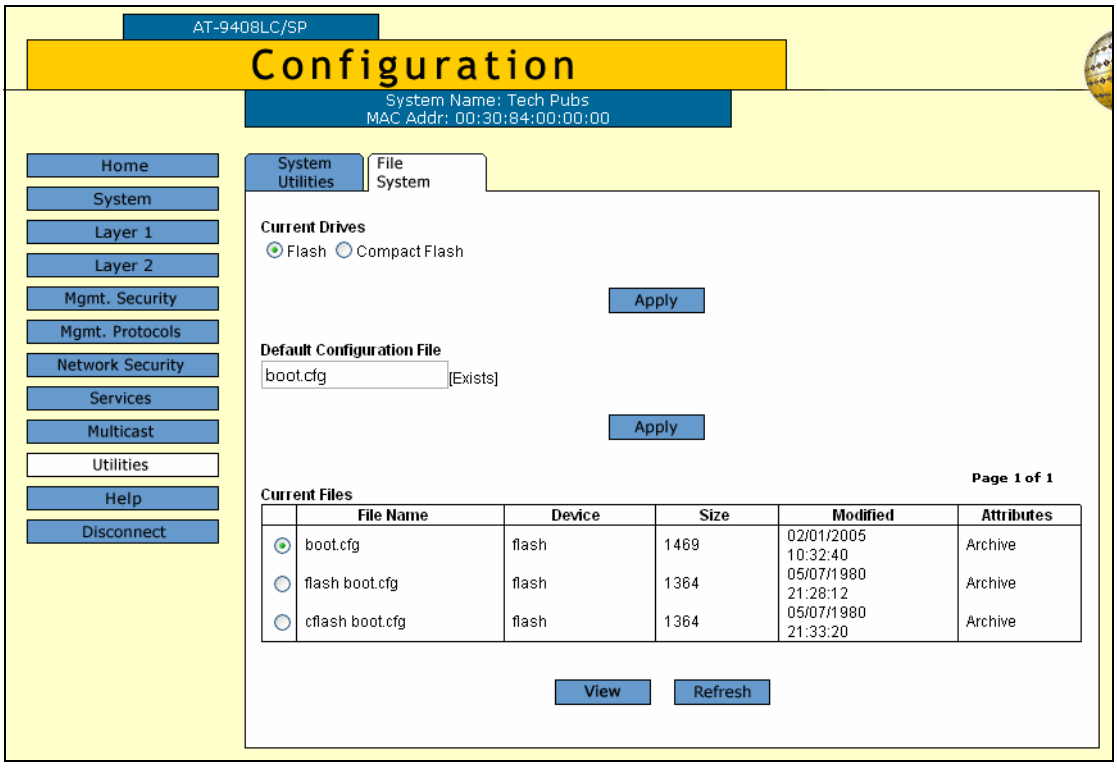

Figure 30. File System Tab (Configuration)

The information in the tab is defined below:

Current Drives
Specifies the location of the files displayed in the Current Files section of the tab. The Flash option represents the switch's flash memory. This is the default selection. The Flash Card option only appears for those AT-9400 Switches that feature a flash card slot.

Default Configuration File
Specifies the filename of the active configuration file. The switch uses this file to configure its operating parameters when reset or power cycled. The switch also updates the active boot file when you select the Save Config option.

The columns in the List Files table are described below. This information is for viewing purposes only. If your unit has a compact flash card slot, the switch, by default, displays the files in flash memory. To view the files on a card, go to step 4.

File Name
Name of the system file.

Device
The device type, either "flash" for flash memory or "cflash" for compact flash card.

Size
Size of the file, in bytes.

Modified
The time the file was created or last modified, in the following date and time format: month/day/year hours:minutes:seconds.

Attributes
The file type, one of the following:

- Normal
- Read Only
- Hidden
- System
- Volume
- Directory
- Archive
- Invalid

4. To view the files on a compact flash card, insert the card into the slot on the switch, select **Compact Flash** under Current Drivers, and click **Apply**.

5. To view the contents of a file, such as a configuration file, click the file in the Current Files section of the tab and click **View**. You can view one file at a time.

   The contents of the configuration file are displayed in the Viewing File page. An example is shown in Figure 31.

   .

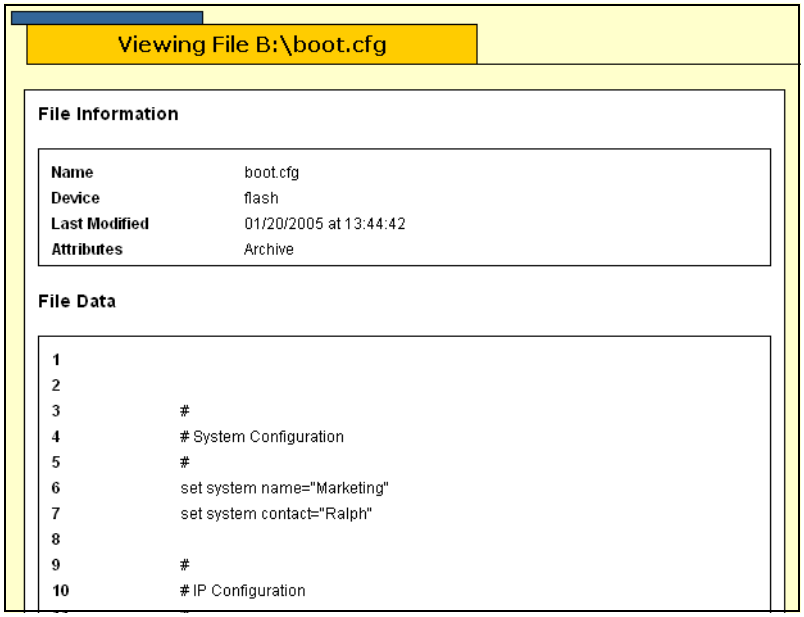

Figure 31. Viewing File Page

Selecting an Active Boot Configuration File

This procedure changes the active boot configuration file on the switch. The switch uses the active boot configuration file to configure its operating parameters whenever it is reset or power cycled. The switch also updates the active boot file whenever you select the Save Config option.

Note the following before performing this procedure:

- You cannot create a new configuration file from a web browser management session. That task must be performed from the menus or command line interface.
- The configuration file must already exist in the switch's file system or on a flash memory card. To view the switch's configuration files, see "Listing the Files in Flash Memory or on a Compact Flash Card" on page 106. Configuration files have a ".cfg" extension.
- Specifying a new active boot configuration file does not change the current operating configuration of the switch. To reconfigure the switch using the configuration of a different active boot configuration file, reset or power cycle the switch at the end of the procedure.
- Selecting Save Config after changing the active configuration file overwrites the settings in the file with the current operating settings of the switch.
- You can specify a configuration file on a flash memory card for those systems that support a flash card. However, the switch does not copy the configuration file to its file system. Instead, it uses and updates the file directly on the card. If you remove the card, the switch will not allow you to save any further configuration changes until you reinsert the flash card or specify another active boot configuration file. Furthermore, removing a flash card and resetting the switch causes the switch to return to its default settings.

To change the switch's active configuration file, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Utilities** option.
3. Select the **File System** tab.

   The File System tab for an AT-9400 series switch with a compact flash card is shown in Figure 30 on page 106.
4. In the Default Configuration File field, enter the name of the file to be the new active configuration file. When entering the file name, note the following:

- ❒ Be sure to include the ".cfg" extension.
- ❒ Precede the name with "cflash:" if the file is stored on a flash card in the switch.

5. Click **Apply**.

   The switch searches the file system or flash memory card for the file. If it finds the file, it displays the file name in the Default Configuration File field along with the word "Exists." The file is now the active boot configuration file on the switch.

   If the switch can not locate the file, it displays the name of the previous boot configuration file. Repeat steps 4 and 5, being sure to enter the name correctly.

6. Do one of the following:

   - ❒ To configure the switch using the parameter settings in this boot configuration file, do **not** select Save Config. Instead, reset or power cycle the switch.
   - ❒ To overwrite the settings in the configuration file with the switch's current operating settings, select **Save Config**.

Chapter 9

File Downloads and Uploads

This chapter explains how to upload and download files, such as a new AT-S63 image file, onto the switch. This chapter contains the following sections:

- “Downloading a File” on page 112
- “Uploading a File” on page 116

Downloading a File

This procedure explains how to download a file from a TFTP server on your network to the switch using the web browser interface. You can download any of the following files:

- AT-S63 image file
- Boot configuration file
- CA certificate

Here are the general guidelines to follow when performing this procedure:

- You must use TFTP to download a file from a web browser management session.
- There must be a node on your network with the TFTP server software.
- The file must be stored on the TFTP server node.
- You should start the TFTP server before you begin the download procedure.
- The switch must have a routing interface on the local subnet from where it will reach the TFTP server. The switch uses the IP address of the interface as its source address when sending packets to the TFTP server. This rule applies to both master and slave switches in an enhanced stack. For a switch without a routing interface, you can download the file from a local management session on the switch using Xmodem or, alternatively, switch to switch.
- You cannot download a private encryption key onto a switch, but you can a public key. However, since the switch can use only those encryption keys it has generated itself, Allied Telesis recommends against downloading any keys onto the switch.
- The web browser interface does not support downloading a file to a compact flash memory card in a switch.

If you are downloading the AT-S63 image file, note these additional guidelines:

- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- Installing a new AT-S63 software image does not change the current configuration of a switch.
- If you are upgrading the AT-9400 Switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device's IP configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtained its IP configuration from a DHCP or BOOTP server, the interface is created

with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

- This procedure gives you the option of downloading the image file into the switch's application block or the file system. The application block is the portion of flash memory reserved for the active AT-S63 image file and is separate from the file system. In most cases, you will probably want to download a new image file directly into the switch's application block so that the unit immediately begins to use it as its new operating software. However, there may be occasions when you may want to download the image file to the file system, with plans to copy it to the application block at a later date. It should be noted, however, that the only way to copy an image file in the file system to the application block is with the LOAD command in the command line interface.

Caution
Installing a new AT-S63 image file into the application block of flash memory will cause a switch reset. Some network traffic may be lost.

If you are downloading a boot configuration file, note these additional guidelines:

- A configuration file should only be downloaded onto the same model of switch from where it originated (for example, AT-9408LC/SP to AT-9408LC/SP). Undesirable switch behavior may result if you download a configuration file onto a switch of a different model (for example, AT-9408LC/SP to AT-9424T/SP).
- A configuration file is downloaded onto the switch without any modifications. If the file contains commands for creating routing interfaces with static IP addresses, downloading the same configuration file onto more than one switch may result in an IP address conflict in your network, where routing interfaces on different switches have the same IP addresses.
- You can download the file as the active boot file for the switch, in which case it automatically becomes the switch's active boot file, or just into the file system. If you choose the latter, you can manually designate the file as the switch's active boot file at a later time.

Caution
Downloading a configuration file as the switch's new active boot configuration file will cause a switch reset. Some network traffic may be lost.

To download a file, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab selected by default, as shown in Figure 32.

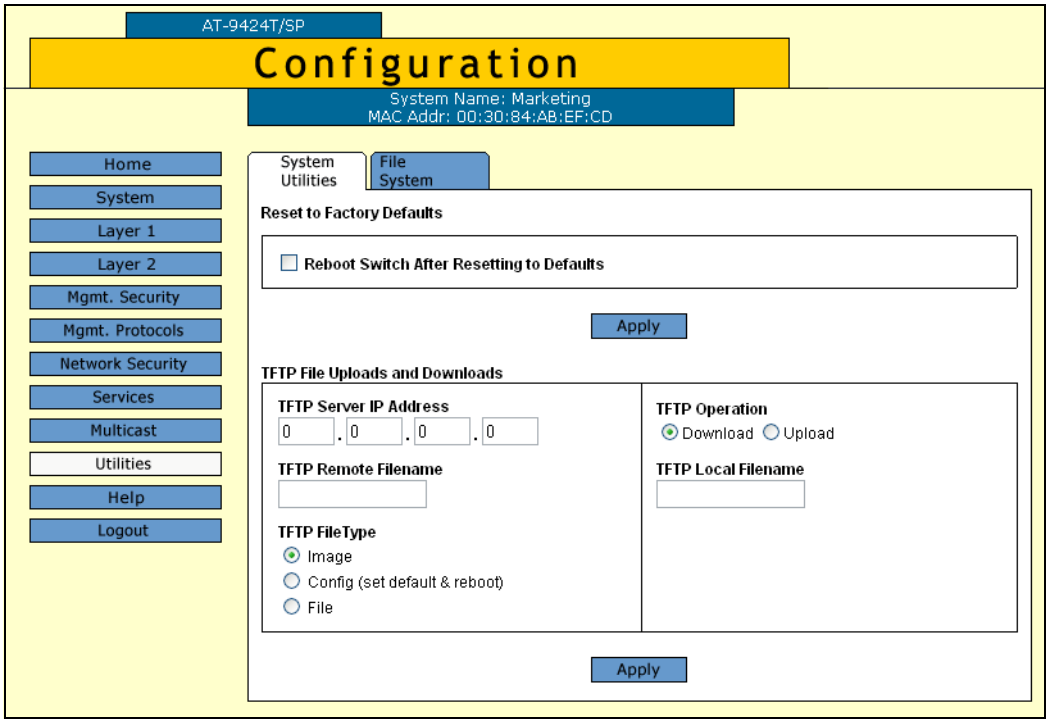

Figure 32. System Utilities Tab (Configuration)

Note
The top portion of the System Utilities tab returns the switch to its factory default settings. For instructions, refer to “Returning the AT-S63 Management Software to the Factory Default Values” on page 37.

3. In the TFTP Server IP Address field, enter the IP address of the network node containing the TFTP server software.
4. For the TFTP Operation parameter, click **Download**.
5. In the TFTP Remote Filename field, enter the filename of the file on the TFTP server to be downloaded to the switch. Be sure to include the filename extension, such as “.img” for an AT-S63 image file or “.cfg” for a configuration file.

6. In the TFTP Local Filename field, enter a name for the file. This is the name the switch uses to store the file in its file system. To download a new AT-S63 image file into the switch's application block, enter "APPBLOCK" as the filename.

7. For the TFTP File Type parameter, select one of the following:

   Image
   Select this option to download a new AT-S63 image file directly into the application block portion of flash memory of the switch so that the device immediately uses it as its active image file.

   Config
   Select this option to download a configuration file that the switch is to immediately employ as its new active boot configuration file.

   File
   Select this option to download a file to the file system, such as a CA certificate or a boot configuration file that is not to be designated as the active boot configuration file.

8. Click **Apply**.

   The management software notifies you after the download is complete.

Caution
When you download a new AT-S63 image file to the switch's application block, the file is written to flash memory. This can require one to two minutes to complete. Do not reset or power off the unit. After the file has been written to flash, the switch automatically resets, ending your web browser management session. Some network traffic may be lost during the reset process. To continue managing the switch, you must reestablish the management session after the reset process is completed.

Note
When you download a configuration file using the Config selection, the file is automatically designated as the switch's new active configuration file. When the download is complete, the switch resets, ending your web browser management session. Some network traffic may be lost during the reset process. After the reset, the switch operates with the parameter settings in the downloaded configuration file. To continue managing the switch, you must reestablish the management session.

Uploading a File

This procedure explains how to upload a file from the switch's file system to a TFTP server on your network using the web browser interface. You can upload any of the following files:

- Boot configuration file
- Public encryption key
- CA enrollment request
- Event log file

Note the following before performing this procedure:

- You must use TFTP to upload a file from a web browser management session.
- There must be a node on your network with the TFTP server software.
- You should start the TFTP server before beginning the upload procedure:
- The switch must have a routing interface on the local subnet from where it will reach the TFTP server. The switch uses the IP address of the interface as its source address when sending packets to the TFTP server. If the switch does not have an interface, you can upload the file from a local management session on the switch using Xmodem.
- The web browser interface does not support uploading a file from a compact flash memory card in the switch to a TFTP server. That type of transfer is supported from the menus and command line interfaces.

To upload a file, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Utilities** option.

   The Utilities page is displayed with the System Utilities tab displayed by default.

   Note
   The top portion of the tab is used to return the switch to its factory default settings. For instructions, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 37.

3. In the TFTP Server IP Address field, enter the IP address of the network node with the TFTP server software.
4. For the TFTP Operation parameter, click **Upload**.

5. In the TFTP Remote Filename field, enter a name for the file when it is stored on the TFTP server.

6. In the TFTP Local Filename field, enter the name of the file in the switch's file system to be uploaded to the TFTP server.

7. In TFTP File Type, select **File**.

   Note
   If you select Image as the TFTP File Type, the switch uploads its active AT-S63 image file to the FTP server and stores it under the name specified in step 5. Allied Telesis does not recommend uploading a switch's image file. If you need an AT-S63 image file to download onto another switch, go to the Allied Telesis web site for the latest version.

8. Click **Apply**.

   The management software notifies you when the upload is complete.

Chapter 10

Event Logs and Syslog Client

This chapter describes how to view switch activity by displaying and saving the contents of the event logs. It also explains how to send events to syslog servers on your network by creating syslog output definitions. Sections in the chapter include:

- ❒ “Working with the Event Logs” on page 120
- ❒ “Working with Syslog Output Definitions” on page 129

Note
The event logs, even when disabled, log all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are entered into the logs only if the event log feature is enabled, which is the default setting for this feature.

Working with the Event Logs

The event logs contain event messages generated by a switch. These events can provide vital information about the operation of the device and can help you identify and resolve network problems. The information includes the time and date when an event occurred, the event's severity, the AT-S63 module that generated the event, and an event description.

The AT-9400 Switch has two event logs. Both logs store the same event messages. There is a temporary log with a storage capacity of 4,000 events. Events in this log are not retained when the switch is reset or power cycled. The other log is in permanent memory with a capacity of 2,000 entries. Events in this log are retained even when the switch is reset or power cycled. You can view either log to display the events of the switch since the unit was last reset. But to view the events that preceded a system reset, you must view the permanent event log.

The following procedures explain how to view the events in the event logs as well as how to enable and disable the logs. The procedures include:

- ❒ "Enabling or Disabling the Event Logs" on page 120
- ❒ "Displaying Events" on page 122
- ❒ "Clearing an Event Log" on page 126
- ❒ "Modifying the Event Log Full Action" on page 127
- ❒ "Saving an Event Log to a File" on page 128

Enabling or Disabling the Event Logs

This procedure explains how to enable and disable the event logs on the switch. If you disable the logs, the AT-S63 Management Software will not store events in its logs or send events to a syslog server. The default setting for the event logs is enabled.

> **Note**
> Allied Telesis recommends setting the switch's date and time if you intend to use the event logs. Otherwise, the entries will not have the correct information when entered in the logs or sent to a syslog server. For instructions, refer to "Setting the System Date and Time" on page 32.

To enable or disable the event logs, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

The Event log tab is shown in Figure 33.

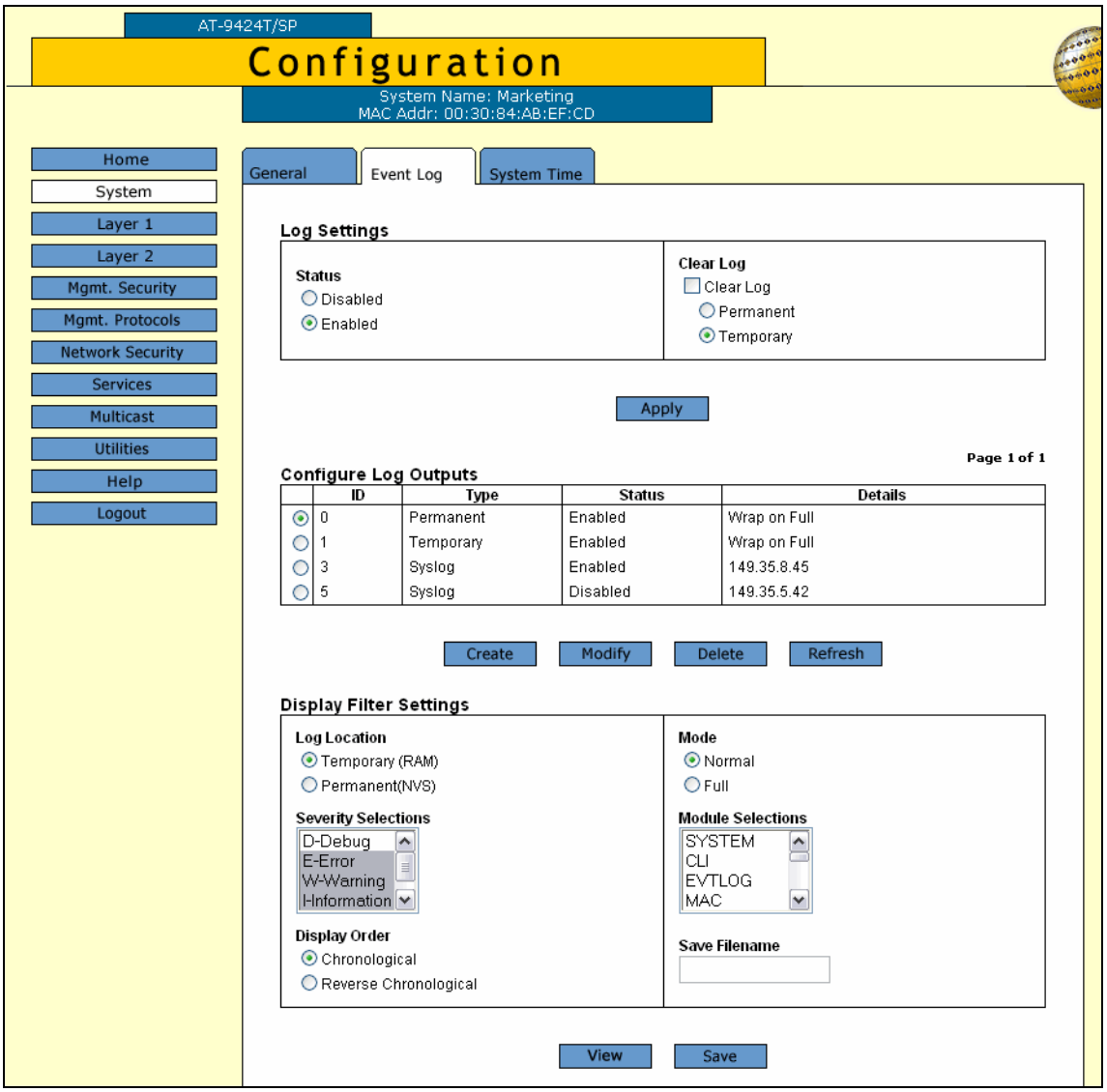

Figure 33. Event Log Tab (Configuration)

4. In the Log Settings section, click **Enabled** for the Status to enable the event logs, or **Disabled** to disable the event logs and to stop the switch from sending events to syslog servers. The default setting is enabled.

5. Click **Apply** to activate the settings on the switch.

   If you enabled the logs, the switch immediately begins to add events to the logs and send events to defined syslog servers.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying Events

This procedure explains how to display the events in an event log. You can view all or just specific events of a log.

To view the events in an event log, perform the following procedure:

1. From the home page, select either **Monitoring** or **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.
4. Configure the parameters in the Display Filter Settings of the tab according to the types of events to be displayed.
5. After configuring the parameters, click **View**.

   The parameters in the Display Filter Settings section are defined here:

   Log Location
   Defines the event log to be viewed: Options are:

   - Temporary (Memory) - Displays the events from the log stored in temporary memory. This log stores approximately 4,000 events. Select this option if the switch has been running for some time without a reset or power cycle. This is the default.
   - Permanent (NVS) - Displays the events from the log stored in nonvolatile memory, which stores up to 2,000 events. Select this option to view the events that occurred prior to a recent reset or power cycle.

   Severity Selections
   Defines the severity of the events to be displayed. You can select more than one severity by using the Ctrl key when making your selections. The default is error, warning, and information events. Options are:

   - D - Debug - Debug messages provide detailed high-volume information only intended for technical support personnel.
   - E - Error - Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.
   - W - Warning - Only warning messages are displayed. These messages indicate that an issue may require manager attention.
   - I - Information - Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.
   - ALL - Messages of all severity levels are displayed.

Display Order
Controls the chronological order of the events in the display. Options are:

- Chronological - Lists the events starting with the oldest events. This is the default.
- Reverse Chronological - Lists the events starting with the most recent events.

Mode
Controls the format of the events in the display. Options are:

- Normal - Displays an event's time of occurrence, module originator, severity, and description for each event. This is the default. An example of Normal mode is shown in Figure 34 on page 125.
- Full - Displays the same information as Normal, plus the file name, line number, and event ID. An example of Full mode is shown in Figure 35 on page 126.

Module Selections
Specifies the AT-S63 software modules whose events will be displayed. The modules are listed in Table 1. You can select more than one module by using the Ctrl key as you make your selections. The default is All.

Table 1. AT-S63 Software Modules

Name	Description
ALL	All modules
ACL	Port access control lists
CFG	Switch configuration file
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
DOS	Denial of Service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP VLAN Registration Protocol
HTTP	Web server
IGMPSNOOP	IGMP snooping

Table 1. AT-S63 Software Modules (Continued)

Name	Description
IP	IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
MLDSNOOP	MLD snooping
PACCESS	802.1X Port-based Access Control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RPS	Redundant power supply
RRP	RRP Snooping
RTC	Real time clock
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	TELNET
TFTP	Trivial File Transfer Protocol
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

Figure 34 shows an example of an event log in Normal mode.

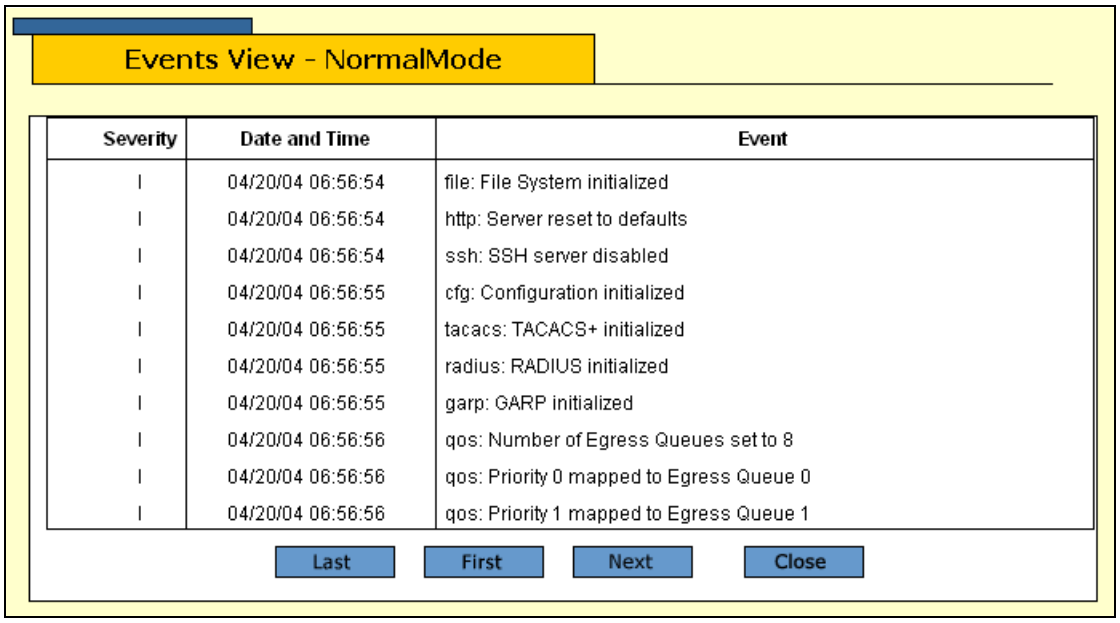
Events View - NormalMode
Severity
Date and Time
Event
I 04/20/04 06:56:54 file: File System initialized
I 04/20/04 06:56:54 http: Server reset to defaults
I 04/20/04 06:56:54 ssh: SSH server disabled
I 04/20/04 06:56:55 cfg: Configuration initialized
I 04/20/04 06:56:55 tacacs: TACACS+ initialized
I 04/20/04 06:56:55 radius: RADIUS initialized
I 04/20/04 06:56:55 garp: GARP initialized
I 04/20/04 06:56:56 qos: Number of Egress Queues set to 8
I 04/20/04 06:56:56 qos: Priority 0 mapped to Egress Queue 0
I 04/20/04 06:56:56 qos: Priority 1 mapped to Egress Queue 1
Last
First
Next
Close

Figure 34. Event Log Example Displayed in Normal Mode

The columns in the table are defined here:

Severity
The event's severity. The severity codes and their corresponding severity level and description are listed in Table 2.

Table 2. Event Severity Levels

Severity Code	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue that may require network manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

Date and Time
The date and time the event occurred.

Event
This item contains two parts. The first is the name of the AT-S63 module that generated the event. The second is a description of the event.

An example of the Full mode is shown in Figure 35.

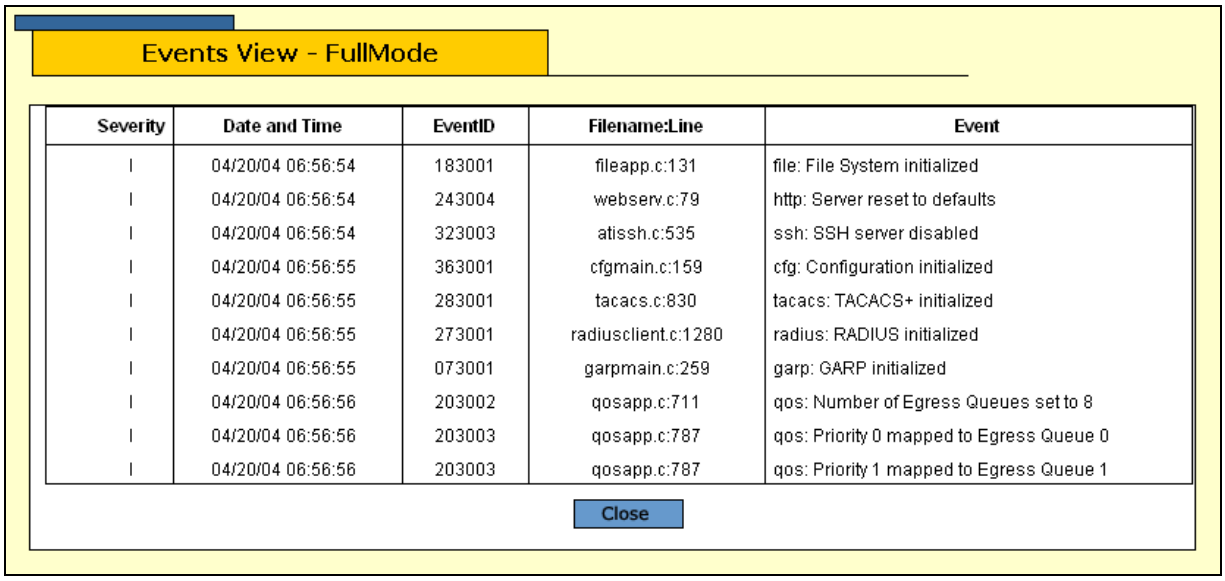
Events View - FullMode
Severity
Date and Time
EventID
Filename:Line
Event
I 04/20/04 06:56:54 183001 fileapp.c:131 file: File System initialized
I 04/20/04 06:56:54 243004 webserv.c:79 http: Server reset to defaults
I 04/20/04 06:56:54 323003 atissh.c:535 ssh: SSH server disabled
I 04/20/04 06:56:55 363001 cfgmain.c:159 cfg: Configuration initialized
I 04/20/04 06:56:55 283001 tacacs.c:830 tacacs: TACACS+ initialized
I 04/20/04 06:56:55 273001 radiusclient.c:1280 radius: RADIUS initialized
I 04/20/04 06:56:55 073001 garpmain.c:259 garp: GARP initialized
I 04/20/04 06:56:56 203002 qosapp.c:711 qos: Number of Egress Queues set to 8
I 04/20/04 06:56:56 203003 qosapp.c:787 qos: Priority 0 mapped to Egress Queue 0
I 04/20/04 06:56:56 203003 qosapp.c:787 qos: Priority 1 mapped to Egress Queue 1
Close

Figure 35. Event Log Example Displayed in Full Mode

The additional information displayed in Full mode is defined here:

Event ID
A unique, random number assigned to each event.

Filename:Line
The originator of the event displayed as the name of the AT-S63 software source file and the line number.

Clearing an Event Log

To clear a log of all events, do the following:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.
4. In the Log Settings section, click the button next to the event log to be cleared, either Permanent or Temporary.
5. Click the **Clear Log** checkbox.
6. Click **Apply**.

   The events in the log are deleted. If the event log feature is enabled, the switch starts to add new events to the log.

Modifying the Event Log Full Action

This procedure controls the action of an event log after reaching its maximum capacity of events. There are two possible actions. In the first action a log deletes the oldest entries as it adds new entries. In the second action the log stops adding entries to preserve the log contents.

Note
The switch continues to send events to syslog servers even when the logs are full.

To configure the event log full action, do the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.
4. Under Current Log Outputs, select Output 0, Permanent, to configure the log in permanent memory, or Output 1, Temporary, to configure the log in temporary memory.
5. Click **Modify**.

   The Modify Event Log Output window is displayed. The window for the temporary memory log is shown in Figure 36.

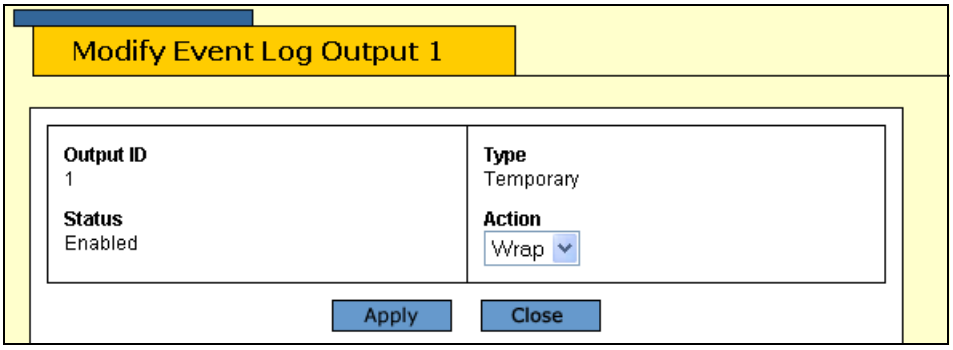

Figure 36. Modifying Event Log Output 1 Window

6. Using the Action pull-down menu, select one of the following:

   Wrap
   The log deletes the oldest entries as it adds new entries after reaching its maximum storage capacity.

   Halt
   The log stops adding new entries to preserve the contents of the log.

7. Click **Apply**.

8. To permanently save the change, select the **Save Config** menu selection.

Saving an Event Log to a File

You can save the current contents of an event log as an ASCII file in the switch's file system. You might save an event log to retain a history of the operation of the switch or to assist in resolving a network problem. The file can be viewed from the file system or uploaded to your management workstation using Xmodem or TFTP.

To save an event log to a file, perform the following procedure:

1. From the home page, select **Configuration**.

2. From the Configuration menu, select the **System** option.

3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.

4. Configure the parameters in the Display Filter Settings section of the tab to define which events in the log are to be saved to the file. For instructions, refer to steps 3 to 7 in "Displaying Events" on page 122.

5. In the Save Filename field, enter a name for the file. The name can be up to 16 alphanumeric characters and must include the ".log" file name extension.

6. Click **Save**.

   The specified events in the log file are saved to the switch's file system as an ASCII file.

7. To view the contents of the file, refer to "Listing the Files in Flash Memory or on a Compact Flash Card" on page 106. To upload the file to a TFTP server, refer to "Uploading a File" on page 116. (To upload the file using Xmodem, you must use a local management session.)

Working with Syslog Output Definitions

You can configure the switch to send its events to a syslog server, which can store the events of many network devices simultaneously. This can make managing your network easier since you need only go to one site, the syslog server, to see all the events of your network devices.

Here are the guidelines to observe when using this feature:

- You can define up to 19 syslog servers.
- The event log feature must be enabled on the switch in order for the device to send events to a syslog server. For instructions, refer to "Enabling or Disabling the Event Logs" on page 120.
- The switch must have a routing interface on the local subnet from where it will reach the syslog server. The switch uses the IP address of the interface as its source address when sending packets to the server.

Configuring the switch to send its events to a syslog server involves creating a syslog output definition. This involves specifying the IP address of the syslog server along with other information, such as the types of event messages the switch is to send to the server.

This section contains the following topics:

- "Configuring a Syslog Output Definition," next
- "Viewing a Syslog Output Definition" on page 132
- "Modifying a Syslog Output Definition" on page 132
- "Deleting a Syslog Output Definition" on page 133

Configuring a Syslog Output Definition

To configure a syslog output file, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.
4. In the Configure Log Outputs section, click **Create**.

The Create Log Output page is shown in Figure 37.

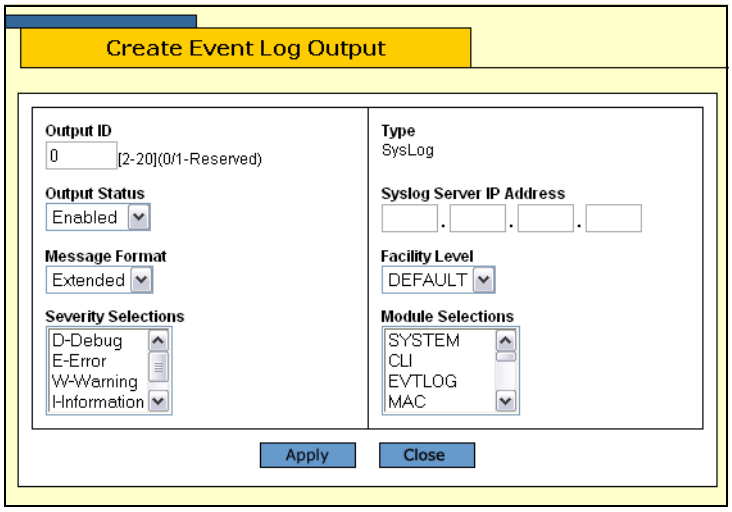

Figure 37. Create Event Log Output Page

5. Configure the following parameters as necessary:

Output ID
Specifies an identification number for the syslog output definition. Each definition must be given a unique number. The range is 2 to 20. The default is the next available number.

Output Status
Controls the status of the syslog output definition. The options are:

Enabled - Enables the output definition. The switch uses the output definition to send events to the syslog server.

Disabled - Disables the log output. The switch does not use the output definition.

Message Format
Controls the format of the sent event messages. The options are:

Extended - Sends the time, module, severity, description, file name, line number, and event ID. This is the default.

Normal - Sends the time, module, severity, and description for each event.

Severity Selections
Specifies the severity of events to be sent to the syslog server. The options are:

ALL - Sends all event messages of the following types. Use Ctrl key to select more than one severity. This is the default.

Error - Sends only error event messages. Error messages indicate that the switch operation is severely impaired.

Warning - Sends only warning event messages. These messages indicate that an issue may require manager attention.

Information - Sends only informational event messages. Informational messages display useful information that you can ignore during normal operation.

Debug - Sends debug event messages. These events provide detailed high-volume information that is intended only for technical support personnel.

Type
Specifies the type of the output definition. The only option is Syslog.

Syslog Server IP Address
Specifies the IP address of the syslog server.

Facility Level
Specifies the numerical code to be added to the entries when sent to the syslog server. The facility levels are listed in Table 3.

Table 3. Default Syslog Facilities

Facility	Mapped Event Log Modules and Events
Default	This setting uses the functional groupings as defined in the RFC 3164 standard.
local 1 through local 7	These settings assign a specific identifier to the events.

Note
For further information about the syslog facility levels, refer to Chapter 12, "Event Logs and Syslog Servers" in the *AT-S63 Management Software Menus Interface User's Guide*.

Module Selections
Specifies the AT-S63 Management Software module(s) whose events are to be sent to the syslog server. To select more than one, use the Ctrl key when making your selections. The default is All. For a list of modules, refer to Table 1 on page 123.

6. Click **Apply**.

   The switch creates the new log output server definition and immediately begins sending events to the server, provided that the Output Status option for the definition is enabled and the log feature on the switch is also enabled.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Viewing a Syslog Output Definition

To view an existing syslog output definition, perform the following procedure:

1. From the home page, select either **Monitoring** or **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event Log tab is shown in Figure 33 on page 121.

4. In the Configured Log Outputs section, select a syslog output from the list and click **View**.

   The View Log Output page is shown in Figure 38.

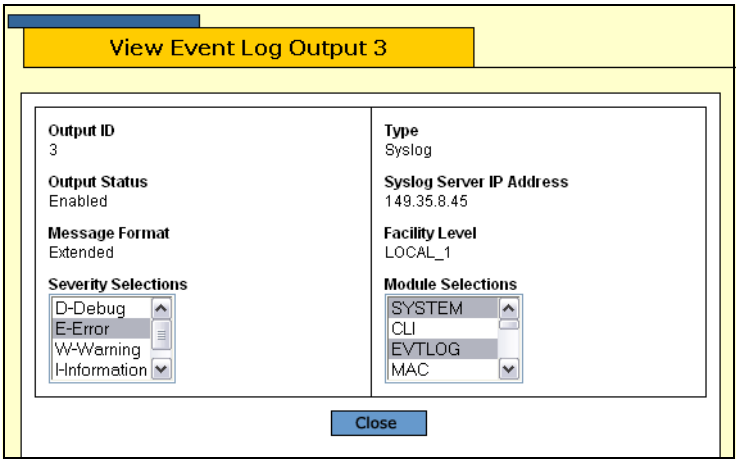

Figure 38. View Event Log Output Page

   For definitions of the parameters, refer to “Configuring a Syslog Output Definition” on page 129.

5. When you are done, click **Close**.

Modifying a Syslog Output Definition

To modify a syslog output definition, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **System** option.
3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.

4. In the Configure Log Outputs section of the tab, select the log output file to be modified and click **Modify**.

   The Modify Event Log Output page is shown in Figure 39.

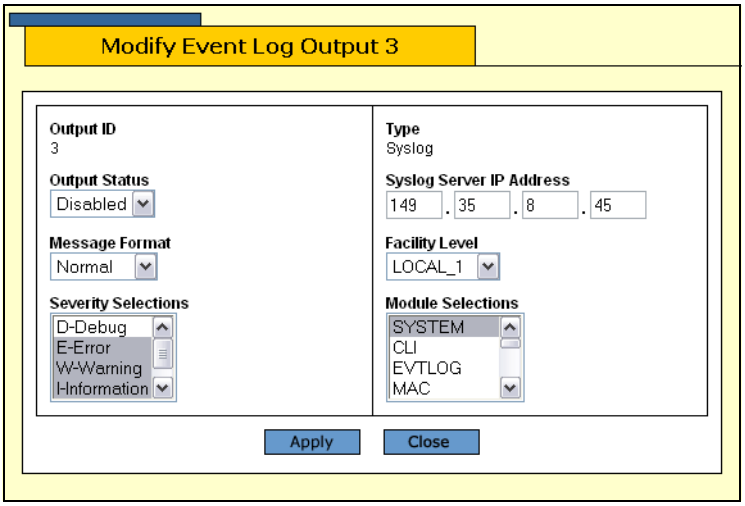

Figure 39. Modify Event Log Output Page

5. Modify the following parameters as necessary. For definitions of the parameters, refer to "Configuring a Syslog Output Definition" on page 129.

6. Click **Apply** to apply the changes or **Close** to close the page without making changes.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Syslog Output Definition

To delete a syslog output definition, perform the following procedure:

1. From the home page, select **Configuration**.

2. From the Configuration menu, select the **System** option.

3. Select the **Event Log** tab.

   The Event log tab is shown in Figure 33 on page 121.

4. In the Configure Log Outputs section, select the syslog output definition to be deleted and click **Delete**.

   The syslog output definition is deleted from the list and the switch stops sending log events to the syslog server.

5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Chapter 11
Classifiers

A classifier defines a traffic flow. Classifiers are used with access control lists (ACLs) to filter ingress traffic on a port and with Quality of Service policies to regulate the traffic flows passing through a switch.

This chapter contains the following sections:

- ❒ “Configuring a Classifier” on page 136
- ❒ “Modifying a Classifier” on page 142
- ❒ “Deleting a Classifier” on page 144
- ❒ “Displaying the Classifiers” on page 145

Configuring a Classifier

To configure a classifier, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** or **Services** option. The Classifier tab is accessible from both menu selections.
3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 40.

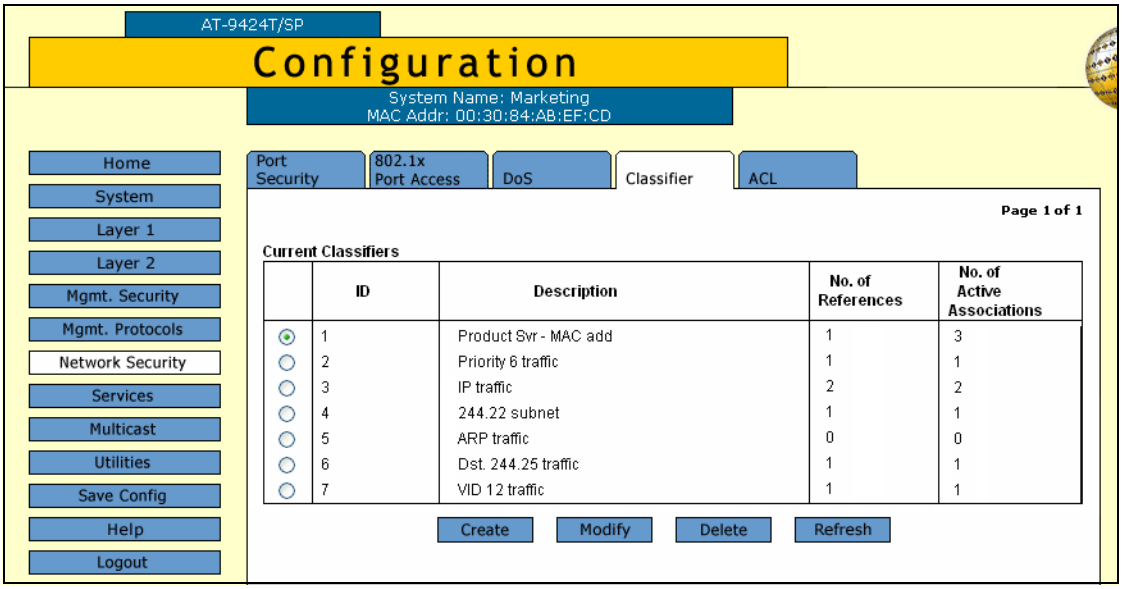

Figure 40. Classifier Tab (Configuration)

The tab lists the current classifiers on the switch. The columns are defined here:

ID
The ID number of the classifier.

Description
A description of the classifier.

No. of References
The number of active and inactive ACLs and QoS policies where the classifier is currently assigned. An active ACL or QoS is assigned to at least one switch port, while an inactive ACL or QoS policy is not assigned to any port. If this column is 0 (zero), the classifier is not assigned to any ACLs or policies, active or inactive.

No. of Active Associations
The number of active ACLs and QoS policies where the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one port.

4. Click **Create**.

   The Create Classifier page is shown in Figure 41.

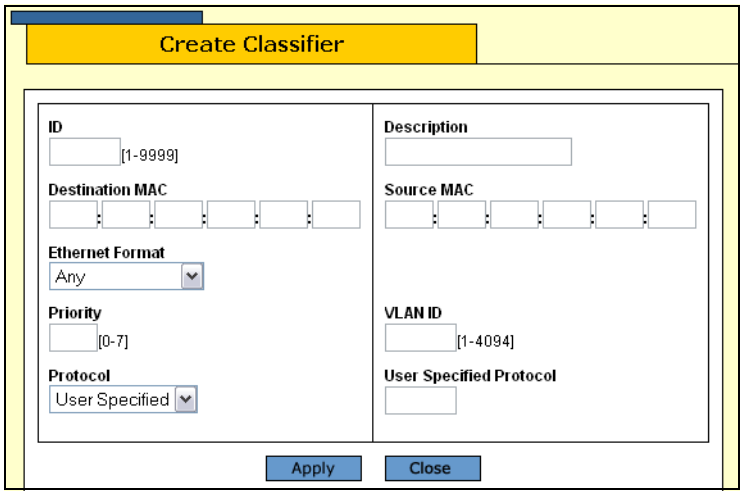

Figure 41. Create Classifier Page

Some of the variables and settings display additional selections. For example, selecting IP as the Protocol displays the selections shown in Figure 42.

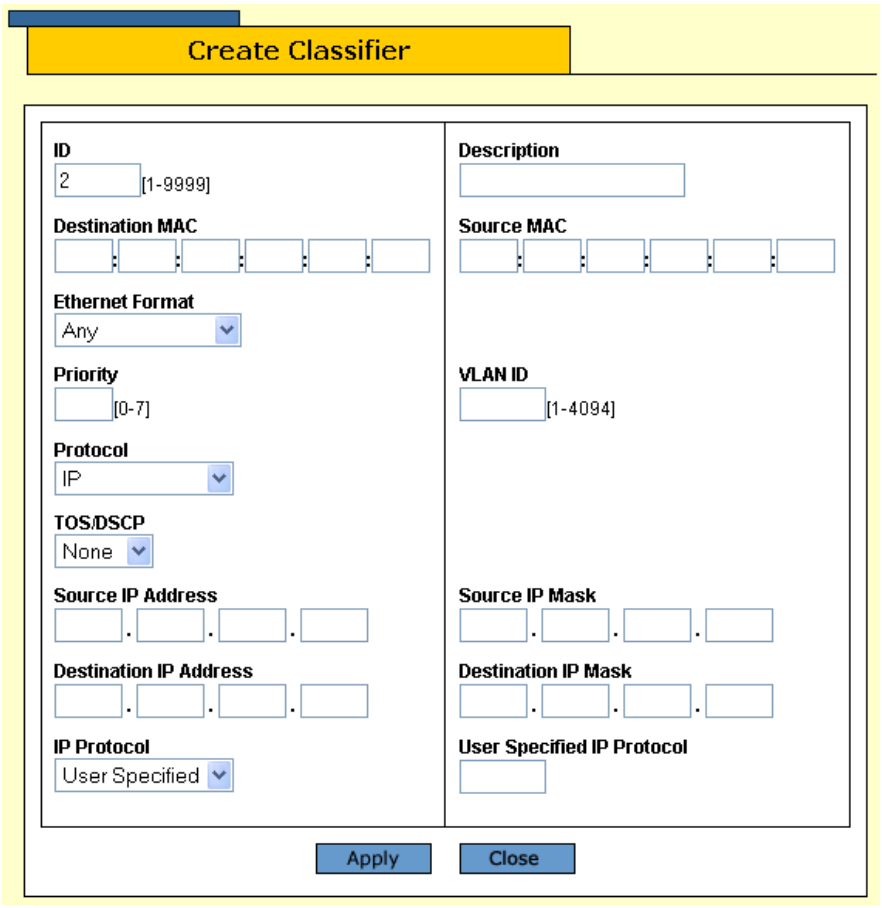

Figure 42. Create Classifier Page - IP Protocol

5. Configure the following parameters as desired:

ID
Specifies an ID number for the classifier. Every classifier on the switch must have a unique ID number. The range is 1 to 9999. This parameter is required.

Description
Specifies a description for the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed.

Destination MAC
Defines a traffic flow by its destination MAC address.

Source MAC
Defines a traffic flow by its source MAC address.

Ethernet Format
Defines a traffic flow by the format of the Ethernet packets. Selections are:

- Untagged - Ethernet II untagged packets
- Tagged - Ethernet II tagged packets
- 802.2 untagged - Ethernet 802.2 untagged packets
- 802.2 tagged - Ethernet 802.2 tagged packets

Priority
Defines a traffic flow by the user priority level in tagged Ethernet frames. The range is 0 to 7.

VLAN ID
Defines a traffic flow of tagged packets by its VLAN ID number. The range is 1 to 4094.

Protocol
Defines a traffic flow by the protocol specified in the Ethertype field of the MAC header in an Ethernet II frame. Possible values are:

- User Specified
- IP
- ARP
- RARP

User Specified Protocol
Defines a traffic flow by the protocol number specified in the Ethertype field of the MAC header in an Ethernet II frame. To use this parameter, the Protocol parameter must be set to User Specified. The number can be entered in either decimal or hexadecimal format. If the latter, precede the number with "0x". The range is 1536 (0x600) to 65535 (0xFFFF).

TOS/DSCP
Defines a traffic flow by its Type of Service or DSCP value. To set this parameter, the Protocol parameter must be set to IP. Options are:

- TOS (Type of Service)
- DSCP

TOS
Defines a traffic flow by its Type of Service value. The range is 0 to 7. To set this value, the TOS/DSCP parameter must be set to TOS.

DSCP
Defines a traffic flow by its DSCP value. The range is 0 to 63. To set this value, the TOS/DSCP parameter must be set to DSCP.

IP Protocol
Defines a traffic flow by the following Layer 3 protocols:

- User Specified
- TCP
- UDP
- ICMP
- IGMP

User Specified IP Protocol
Defines a traffic flow of an Layer 3 protocol by its protocol number. To set this parameter, the IP Protocol parameter must be set to User Specified. The number can be entered in either decimal or hexadecimal format. If the latter, precede the number with “0x”. The range is 0 (0x0) to 255 (0xFF).

Source IP Address
Source IP Mask
Defines a traffic flow by a source IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask “255.255.255.0”.

Destination IP Address
Destination IP Mask
Defines a traffic flow by its destination IP address. The address can be of a specific node or a subnet.

You do not need to include a source IP mask if you are filtering on the IP address of a specific end node. A mask is required, however, when filtering on a subnet. A binary “1” indicates the switch should filter on the corresponding bit of the IP address, while a “0” indicates that it should not. For example, the Class C subnet address 149.11.11.0 would have the mask “255.255.255.0”.

TCP Source Port
Defines a traffic flow by source TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Destination Port
Defines a traffic flow by destination TCP port. To set this parameter, IP Protocol must be set to TCP.

TCP Flags
Defines a traffic flow by TCP flag. To set this parameter, IP Protocol must be set to TCP. Options are

- URG - Urgent
- ACK - Acknowledgement
- RST - Reset
- PSH - Push
- SYN - Synchronization
- FIN - Finish

UDP Source Port
Defines a traffic flow by source UDP port. To set this parameter, IP Protocol must be set to UDP.

UDP Destination Port
Defines a traffic flow by a destination UDP port. To set this parameter, IP Protocol must be set to UDP.

6. Click **Apply**.

   The new classifier is created on the switch.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Classifier

This procedure explains how to modify a classifier.

> **Note**
> If the classifier to be modified is currently assigned to an ACL or QoS policy that has been assigned to a switch port, you must remove the port assignments from the ACL or policy before you can modify the classifier. After you have finished modifying the classifier, you can reassign the ports again to the ACL or QoS policy.

To modify a classifier, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** or **Services** option. The Classifier tab is accessible from both menu selections.
3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 40 on page 136.
4. Click the dialog circle next to the classifier to be modified and click **Modify**. You can modify only one classifier at a time. An example of the Modify Classifier page is shown in Figure 43.

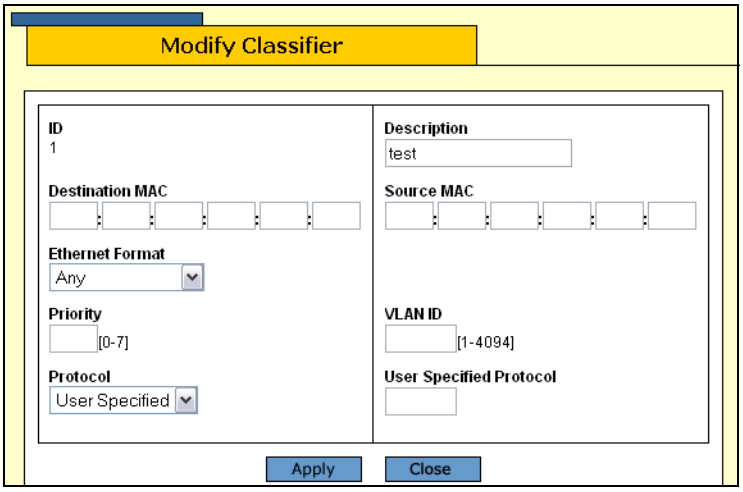

Figure 43. Modify Classifier Page

5. Modify the parameters as necessary. For parameter descriptions, refer to “Configuring a Classifier” on page 136.

6. When you are finished modifying the parameters, click **Apply**. The modifications are immediately implemented in the classifier.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Classifier

To delete a classifier, perform the following procedure:

Note
A classifier must be removed from all access control lists and QoS policies before it can be deleted.

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** or **Services** option. The Classifier tab is accessible from both menu selections.
3. Select the **Classifier** tab.

   The Classifier tab is shown in Figure 40 on page 136.
4. Click the button next to the classifier to be deleted and click **Delete**. Only one classifier can be deleted at a time.

   The classifier is deleted from the switch.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Classifiers

To display the classifiers, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Configuration menu, select the **Network Security** or **Services** option. The Classifier tab is accessible from both menu selections.
3. Select the **Classifiers** tab.

   The Classifiers tab is shown in Figure 44.

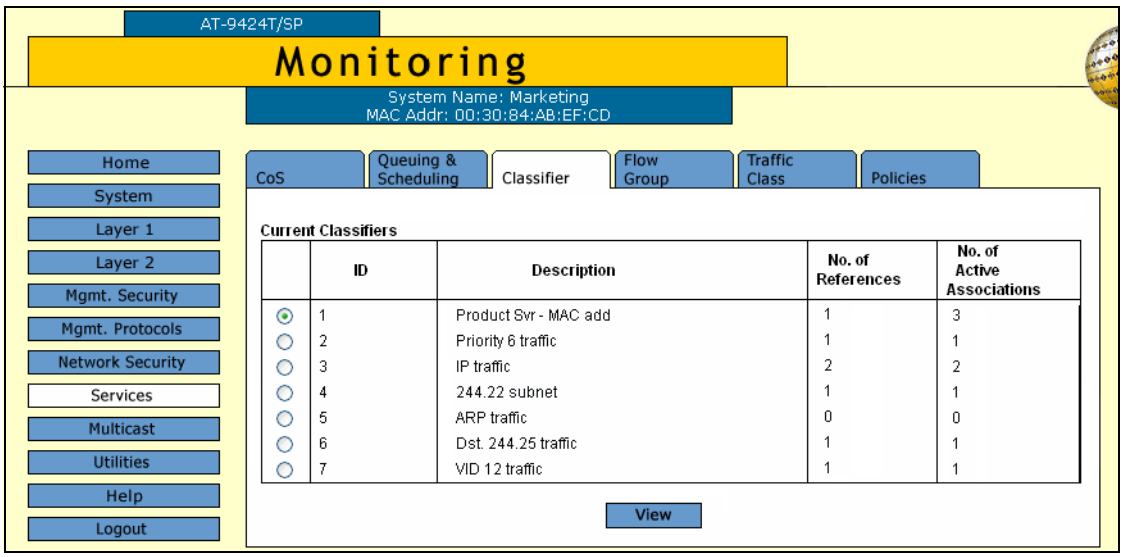

Figure 44. Classifier Tab (Monitoring)

The Classifier tab displays a table of the currently configured classifiers that contains the following columns of information:

ID
The ID number of the classifier.

Description
A description of the classifier.

No. of References
The number of active and inactive ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS is assigned to at least one switch port, while an inactive ACL or QoS policy is currently not assigned to any port. If this column is 0 (zero), the classifier is not assigned to any ACLs or policies, active or inactive.

No. of Active Associations
The number of active ACLs and QoS policies to which the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch.

4. To display detailed information about a classifier, select the classifier and click **View**.

   For descriptions of the variables, refer to “Configuring a Classifier” on page 136.

5. Click **Close** to close the page.

Chapter 12

Access Control Lists

An access control list (ACL) is a tool for managing network traffic. This chapter contains the following sections:

- ❒ “Configuring an Access Control List” on page 148
- ❒ “Modifying an Access Control List” on page 151
- ❒ “Deleting an Access Control List” on page 152
- ❒ “Displaying the Access Control Lists” on page 153

Configuring an Access Control List

This procedure explains how to create an ACL. Before starting this procedure, jot down on paper the ID number(s) of the classifier(s) to be assigned to the ACL. This information will make it easier for you to perform the procedure. To view the classifier ID numbers and specifications, refer to “Displaying the Classifiers” on page 145.

To configure an access control list, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 45.

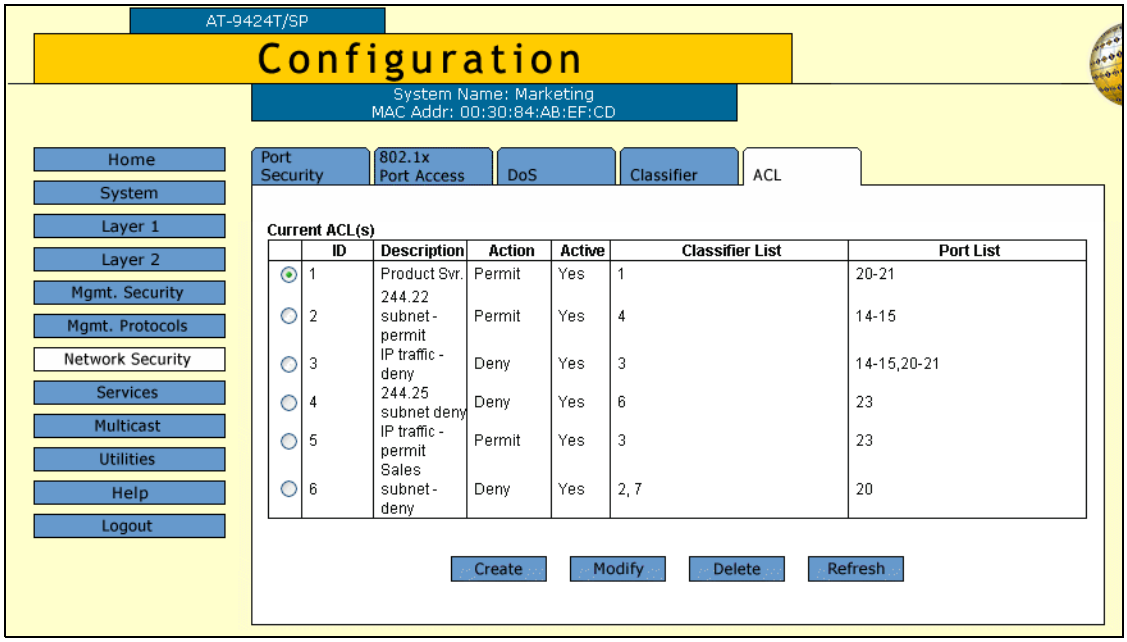

Figure 45. ACL Tab (Configuration)

The Current ACL(s) section of the tab displays a table of the existing ACLs. The table has the following columns of information:

ID
The ID number of the ACL.

Description
A description of the ACL.

Action
The ACL action of Permit or Deny. An action of Permit means the port

accepts the packets that meet the criteria of the classifiers assigned to the ACL. An action of Deny means the port discards the packets, unless the packets also match the criteria of a Permit ACL, in which case the packets are accepted by the port, because a Permit ACL overrides a Deny ACL.

Active
Whether or not the ACL is active. A status of Yes means that the ACL is assigned to at least one port on the switch. A status of No means the ACL is not assigned to any ports and therefore is inactive.

Classifier List
The classifiers assigned to the ACL.

Port List
The port assignments of the ACL.

4. To create a new ACL, click **Create**.

   The Create ACLs page is displayed, as shown in Figure 46.

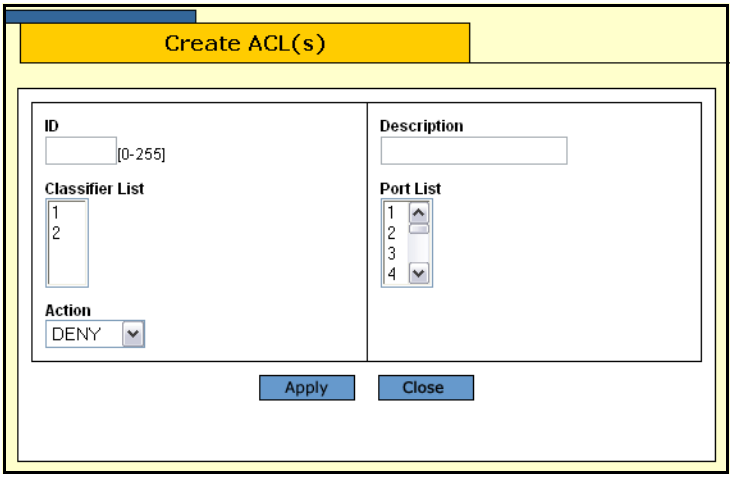

Figure 46. Create ACLs Page

5. Configure the following parameters:

   ID
   Use this field to enter an ID number for the ACL. Every ACL on the switch must have a unique ID number. The range is 0 to 255.

   Classifier List
   Use the list to select the classifier to be assigned to the ACL. You can assign more than one classifier to an ACL. To select multiple classifiers, hold down the Ctrl key while making your selections. To view the classifiers on a switch, refer to "Displaying the Classifiers" on page 145. An ACL must have at least one classifier.

Action
Use this menu to specify the action of the ACL. An action of Permit means the port accepts the packets that meet the criteria of the classifiers assigned to the ACL. An action of Deny means the port discards the packets, unless the packets also match the criteria of a Permit ACL, in which case the packets are accepted by the port, because a Permit ACL overrides a Deny ACL.

Description
Use this field to enter a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces. A description is optional.

Port List
Use this list to specify the port where the ACL is to be assigned. You can assign an ACL to more than one port. To select multiple ports, hold down the Ctrl key while making your selections. You do not have to assign an ACL to a port when you initially create it. However, an ACL remains inactive until it is assigned to a port.

6. Click **Apply**.

   The new ACL is immediately activated on the specified ports. If you did not specify any ports for the ACL, the ACL is created but remains inactive until you assign it to a port.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying an Access Control List

To modify an access control list, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 45 on page 148.
4. Select the ACL to be modified and click **Modify.**

   The Modify ACLs page is displayed, as shown in Figure 47.

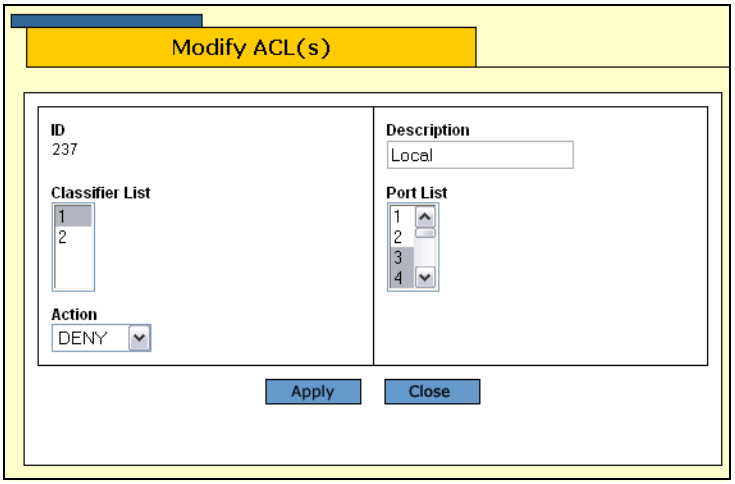

Figure 47. Modify ACLs Page

5. Configure the parameters as needed. For definitions of the parameters, refer to "Configuring an Access Control List" on page 148.
6. Click **Apply.**

   Changes to the ACL are immediately implemented on the switch.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting an Access Control List

To delete an access control list, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 45 on page 148.
4. Select the ACL to be deleted and click **Delete**. You can delete one access control list at a time.

   The ACL is immediately deleted from the switch.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Access Control Lists

To display the current ACLs, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Network Security**.
3. Select the **ACL** tab.

   The ACL tab is shown in Figure 48.

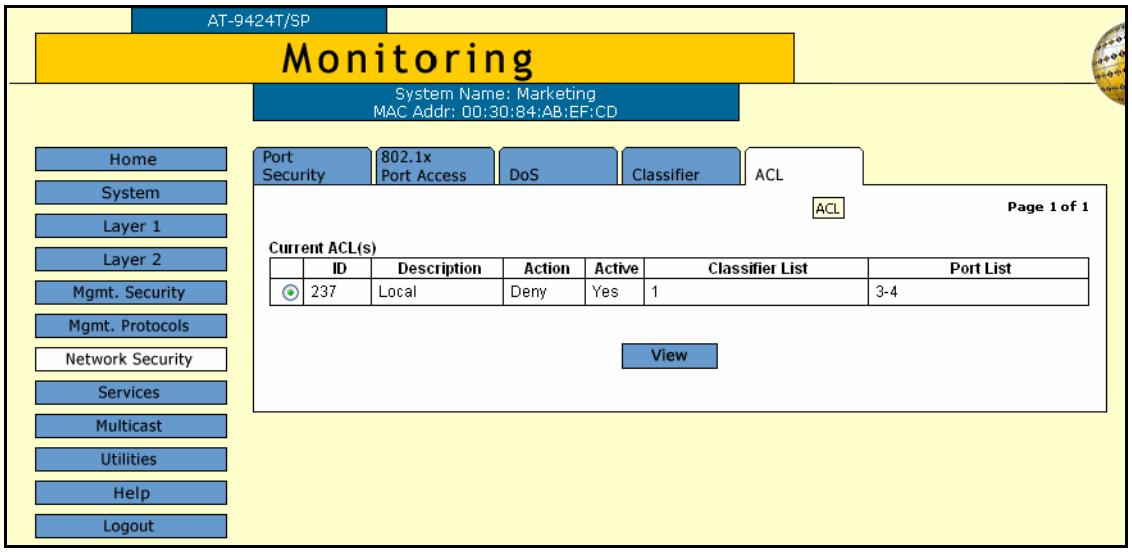

Figure 48. ACL Tab (Monitoring)

The ACL tab displays a table of the currently configured ACLs with the following columns of information:

ID
The ID number for the ACL.

Description
A description of the ACL.

Action
The ACL action of Permit or Deny. An action of Permit means the port accepts the packets that meet the criteria of the classifiers assigned to the ACL. An action of Deny means the port discards the packets, unless the packets also match the criteria of a Permit ACL, in which case the packets are accepted by the port, because a Permit ACL overrides a Deny ACL.

Active
Whether or not the ACL is active. A status of Yes means that the ACL

is assigned to at least one port on the switch. A status of No means the ACL is not assigned to any ports and therefore is inactive.

Classifier List
The classifiers assigned to the ACL.

Port List
The port assignments of the ACL.

4. To view the same information for each ACL, select the ACL and click **View.**

   The View ACLs page opens, as shown in Figure 49.

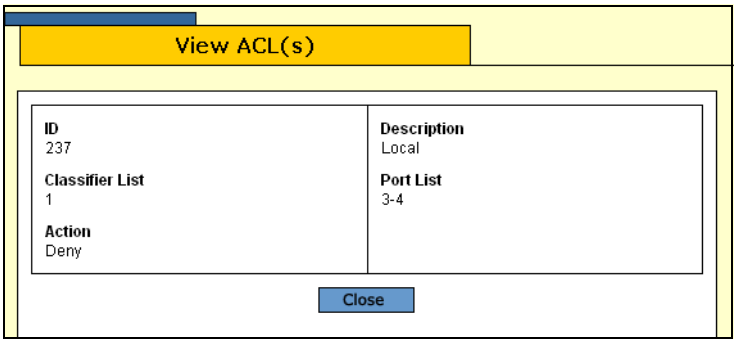

Figure 49. View ACLs Page

5. Click **Close**.

Chapter 13

Class of Service

This chapter contains instructions on how to configure Class of Service (CoS). This chapter contains the following procedures:

- ❒ “Configuring CoS” on page 156
- ❒ “Mapping CoS Priorities to Egress Queues” on page 158
- ❒ “Configuring Egress Scheduling” on page 160
- ❒ “Displaying the CoS Settings” on page 161
- ❒ “Displaying the QoS Schedule” on page 163

Configuring CoS

This procedure sets the Class of Service priority level for ingress untagged packets on a port. The priority level dictates which priority queue the packets are stored in on the egress port. In the default settings, ingress untagged packets on a port are assigned a priority level of 0 and are stored in egress queue Q1 on the egress port. This procedure also overrides the priority level in tagged ingress packets. To adjust the mappings of priority levels to egress queues, refer to “Mapping CoS Priorities to Egress Queues” on page 158.

To change the CoS priority level on a port, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 50.

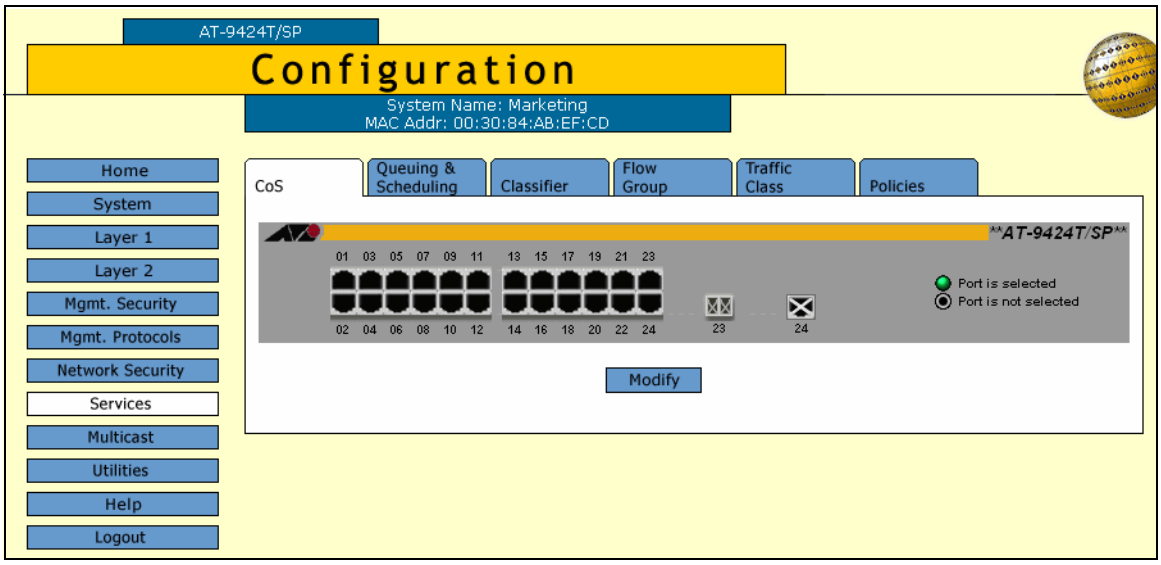

Figure 50. CoS Tab (Configuration)

3. Select the ports whose CoS settings are to be configured and click **Modify**.

The CoS Setting for Port page is shown in Figure 51.

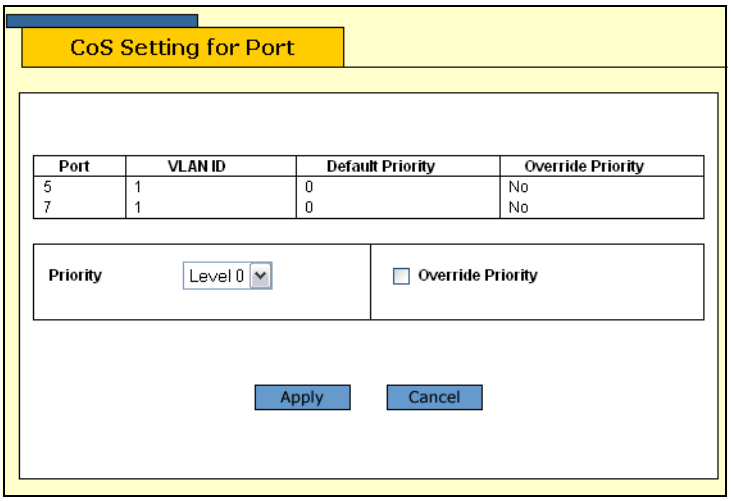

Figure 51. CoS Setting for Port Page

4. Use the Priority list to select a new Class of Service priority level for the port. The default is level 0. The new priority level will apply to all ingress untagged packets. (If you perform Step 5 and override the priority level in tagged packets, the new priority level will also apply to all ingress tagged packets.)

5. If you are configuring a tagged port and you want the port to ignore the priority tag in the packets, click the **Override Priority** option. A check in the box indicates this feature is activated. All tagged packets are directed to the egress queue specified in Step 4.

   Note
   The switch does not change the tagged information in a tagged packet. A tagged packet exits the switch with the same priority level that it had when it entered.

   The default for this parameter is No, meaning that the priority level of a tagged packet is determined by the tagged information in the packet itself.

6. Click **Apply**.

   Configuration changes are immediately activated on the switch.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues. To change the mappings, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Queuing & Scheduling** tab.

   The Queuing & Scheduling tab is shown in Figure 52.

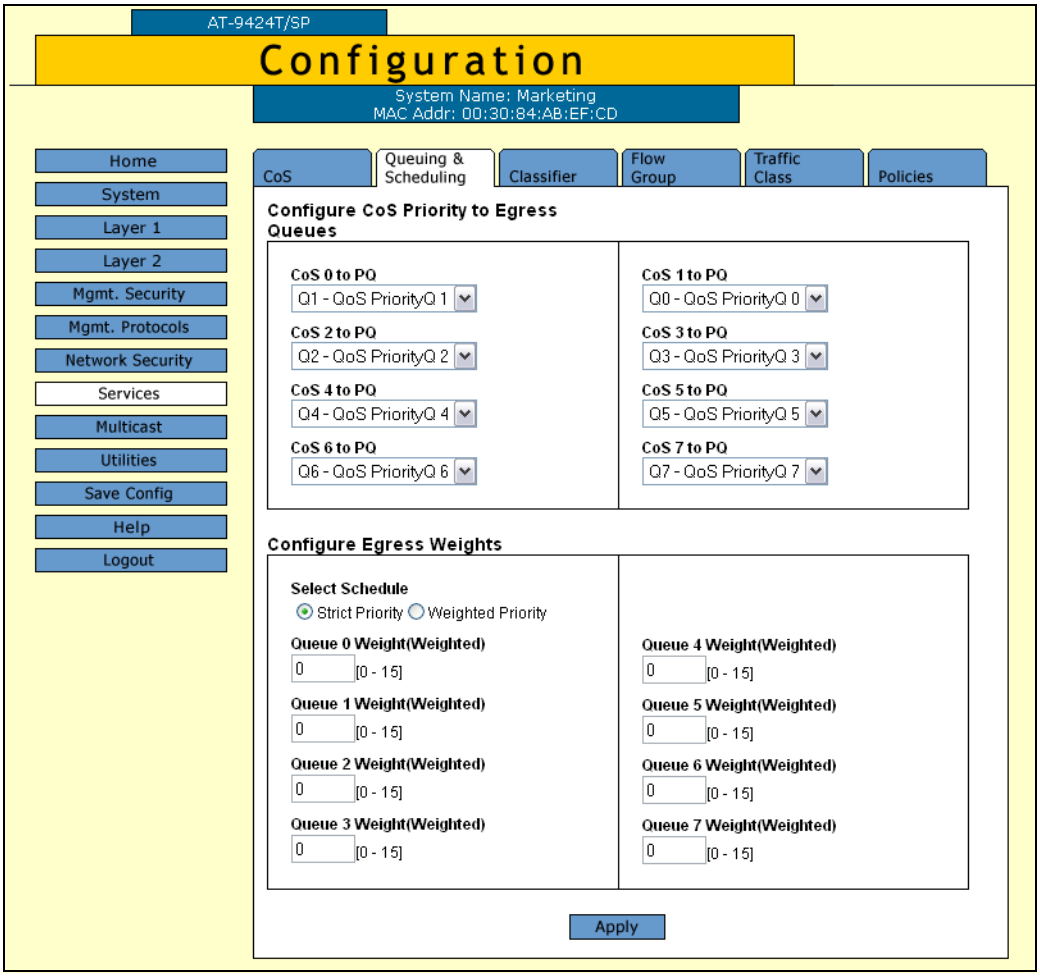

Figure 52. Queuing & Scheduling Tab (Configuration)

Note
The Configure Egress Weights section in the tab is explained in the next procedure, “Configuring Egress Scheduling” on page 160.

The default values are listed in Table 4.

Table 4. Default Mappings of IEEE 802.1p Priority Levels to Egress Priority Queues

IEEE 802.1p Priority Level	Egress Port Priority Queue
0	Q1
1	Q0
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7

4. In the Configure CoS Queues to Egress Queues section of the tab, click the list for a CoS priority whose queue assignment is to be changed and select the new queue.

   For example, to direct all ingress tagged packets with a CoS priority of 5 to egress queue Q3, you would use the list in **CoS 5 to PQ** and select **Q3 - QoS PriorityQ 3.**

5. If desired, repeat Step 4 to change the egress queue assignment of other CoS priorities.

6. Click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring Egress Scheduling

This procedure explains how to select and configure a scheduling method for Class of Service. Scheduling determines the order in which the ports handle packets in their egress queues. For an explanation of the two scheduling methods, refer to the *AT-S63 Management Software Features Guide*. Scheduling is set at the switch level. You can not set this at the port level.

To change scheduling, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Queuing & Scheduling** tab.

   The Queuing & Scheduling tab is shown in Figure 52 on page 158.

   Note
   The Configure CoS Queues to Egress Queues section in the tab is explained in the previous procedure “Mapping CoS Priorities to Egress Queues” on page 158.

4. To select a scheduling method, click either **Strict Priority** or **Weighted Priority** in the Configure Egress Weights section of the tab. The default is Strict Priority.

   Skip the next step if you select Strict Priority. Queue weights do not apply to Strict Priority scheduling.

5. If you selected Weighted Priority, use the Queue # Weight fields to specify the maximum number of packets a port can transmit from an egress queue before going to the next queue. The range for Q0 to Q6 is 1 to 15 packets. The range for Q7 is 0 to 15 packets. A setting of 0 of Q7 means that its packets always take priority over the packets in the other queues, and that packets are transmitted from the other queues only when Q7 is empty.

   The default setting for all queues is 1. At the default setting, all queues have the same weight.

6. Click **Apply**.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the CoS Settings

To display the CoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Services**.

   The Services page is displayed with the CoS tab selected by default, as shown in Figure 53.

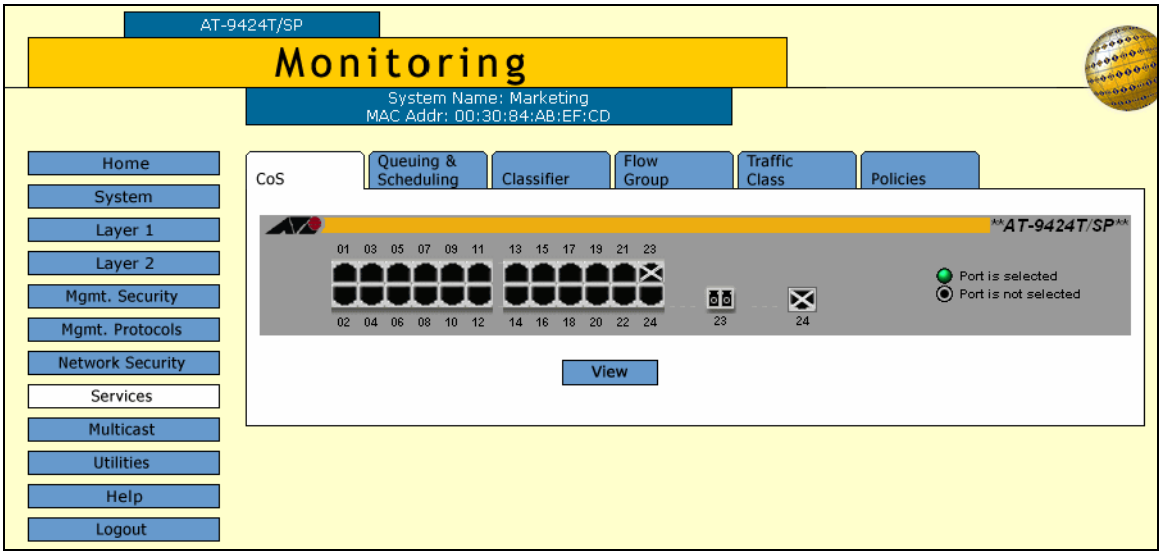

Figure 53. CoS Tab (Monitoring)

3. Click the port whose settings are to be displayed. You can select more than one port. A selected port turns white. (To deselect a port, click it again.)
4. Click **View**.

   The CoS Setting for Port page is shown in Figure 54.

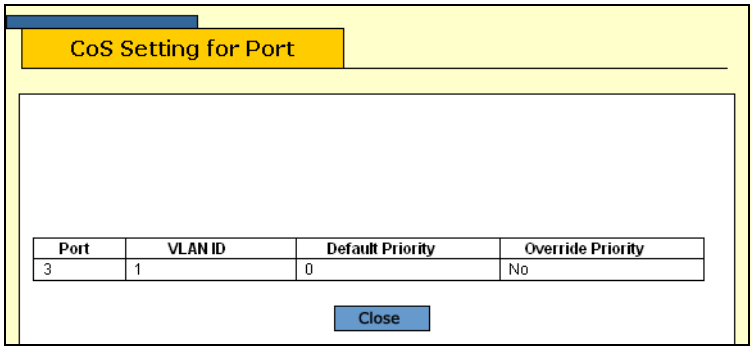

Figure 54. CoS Setting for Port Page

The CoS Setting for Port page displays a table that contains the following columns of information:

Port
The port number.

VLAN ID
The VLAN where the port is an untagged member.

Default Priority
The default priority level assigned to ingress untagged packets on this port.

Override Priority
Whether the priority level in tagged packets should be overridden.

5. Click **Close**.

Displaying the QoS Schedule

To display the QoS schedule, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Services** option.
3. Select the **Queuing and Scheduling** tab.

   The Queuing and Scheduling tab is shown in Figure 55.

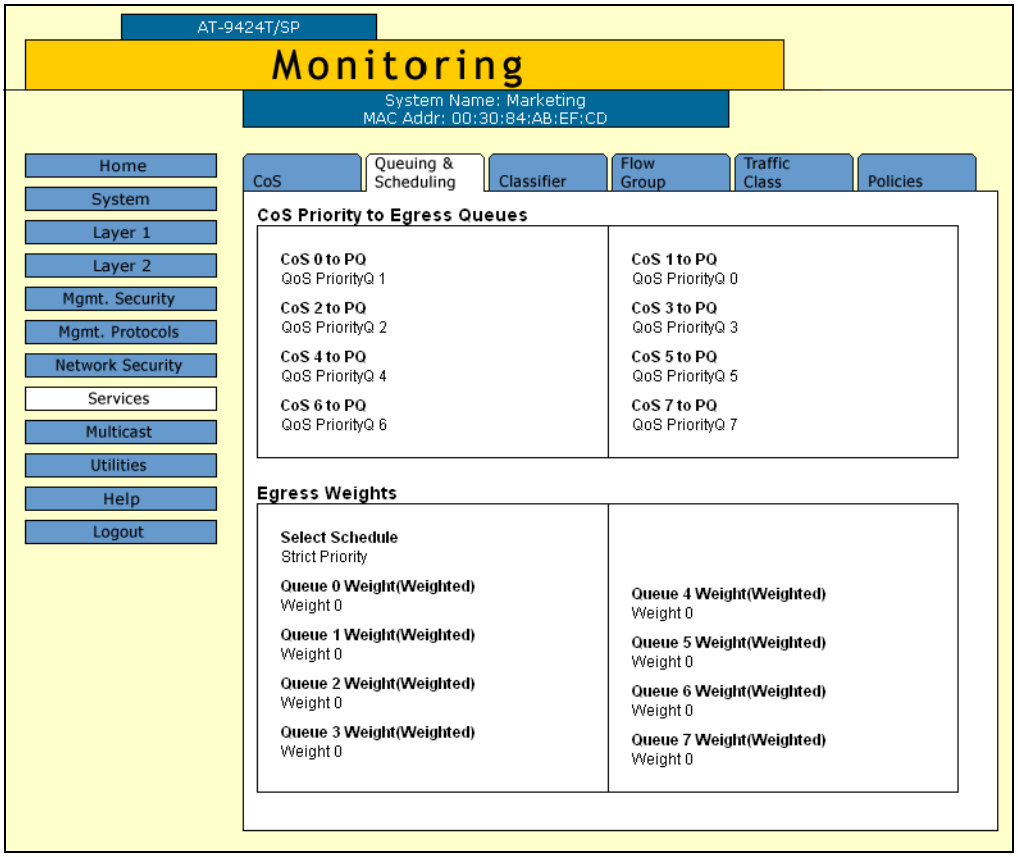

Figure 55. QoS Scheduling Tab (Monitoring)

The upper section displays the CoS priority to egress queue assignments. The lower section displays the egress weight settings.

Chapter 14

Quality of Service

This chapter contains instructions on how to configure Quality of Service (QoS). This chapter contains the following procedures:

- ❒ “Managing Flow Groups” on page 166
- ❒ “Managing Traffic Classes” on page 172
- ❒ “Managing Policies” on page 180

Managing Flow Groups

This section contains the following procedures:

- ❒ “Configuring a Flow Group,” next
- ❒ “Modifying a Flow Group” on page 169
- ❒ “Deleting a Flow Group” on page 170
- ❒ “Displaying the Flow Groups” on page 170

Configuring a Flow Group

To configure a flow group, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 56.

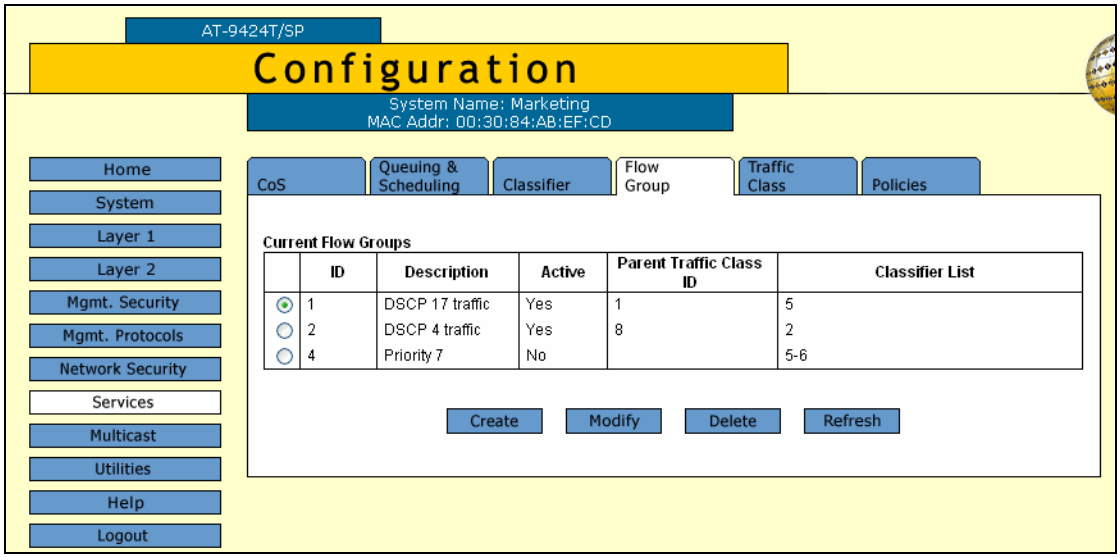

Figure 56. Flow Group Tab (Configuration)

The columns in the tab are defined here:

ID
The ID number of the flow group.

Description
The flow group description.

Active
The active status of the flow group. A flow group is deemed active if it is part of a policy assigned to a switch port. A flow group is considered

inactive if it is not a part of any policies or if the policies are not assigned to any ports.

Parent Traffic Class ID
The traffic class where the flow group is assigned.

Classifier List
The classifiers of the flow group.

4. Click **Create**.

   The Create Flow Group page opens, as shown in Figure 57.

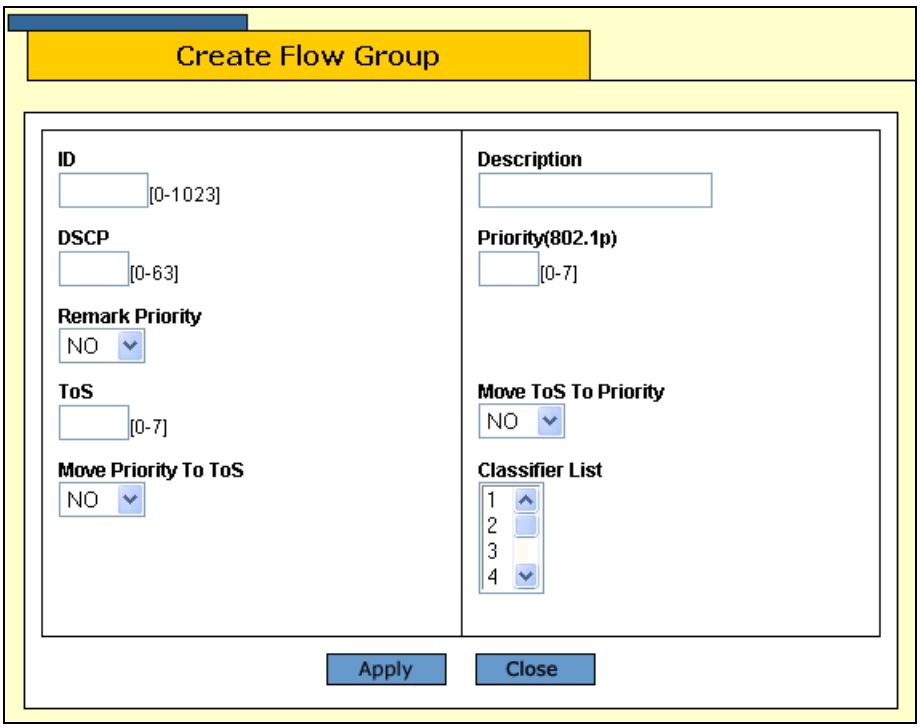

Figure 57. Create Flow Group Page

5. Configure the following parameters as necessary:

   ID
   Specifies the ID number for this flow group. A flow group must be assigned a unique ID number. The range is 0 to 1023.

   Description
   Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

   DSCP
   Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value

specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

Priority (802.1p)
Specifies a new user priority value for the packets. The range is 0 to 7. You can specify a new priority value at both the flow group and traffic class levels. If you specify a new user priority value at both levels, the value in the flow group here overrides the value in Traffic Class. If you want the packets to retain the new value when they exit the switch, change Remark Priority to Yes.

Remark Priority
If set to Yes, replaces the user priority value in the packets with the new value specified in the Priority parameter when the packet leaves the switch.

ToS
Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

Move ToS to Priority
Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no Does not replace the preexisting 802.1p priority level. This is the default.

Move Priority to ToS
Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no Does not replace the ToS priority field. This is the default.

Classifier List
Lists the classifiers on the switch. You use the list to specify the classifier for the flow group. The classifier must already exist on the switch. A flow group can be assigned more than one classifier. To select more than one classifier, hold down the Ctrl key when making your selections.

6. Click **Apply**.

   The management software creates the new flow group.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Flow Group

This procedure explains how to modify a flow group. If the flow group is already part of a QoS policy assigned to one or more switch ports, you must modify the policy by removing the port assignments before you can modify the flow group. You can reassign the ports back to the policy after modifying the flow group.

To modify a flow group, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 56 on page 166.

4. Click the dialog circle next to the flow group to be modified and click **Modify**. You can modify only one flow group at a time.

   The Modify Flow Group page is displayed, as shown in Figure 58.

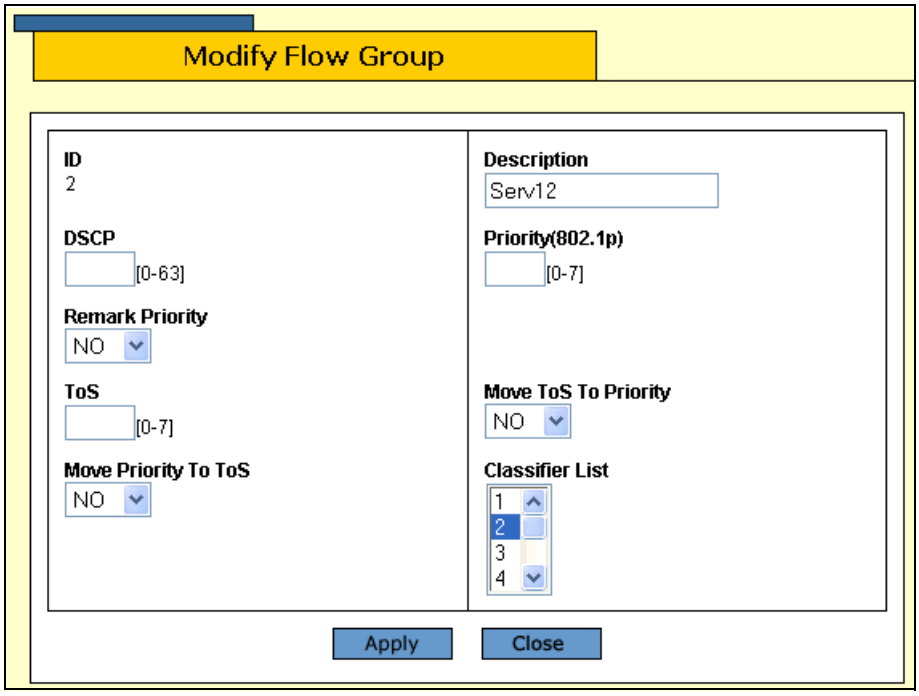

Figure 58. Modify Flow Group Page

5. Modify the parameters as necessary. For definitions, refer to "Configuring a Flow Group" on page 166.
6. Click **Apply**.

The changes are applied to the flow group.

7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Flow Group

This procedure explains how to delete a flow group. If the flow group to be deleted is already part of a QoS policy assigned to one or more switch ports, you must modify the policy by removing the port assignments before you can delete the flow group. You can assign the ports back to the policy after you have deleted the flow group.

To delete a flow group, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Flow Group** tab.

   The Flow Group tab is shown in Figure 56 on page 166.

4. Select the flow group to be deleted and click **Delete**.

   The flow group is deleted from the switch.

5. To permanently save your changes, select the **Save Config** menu selection.

Displaying the Flow Groups

To display the flow groups, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Services** option.
3. Select the **Flow Group** tab.

The Flow Group tab is shown in Figure 59.

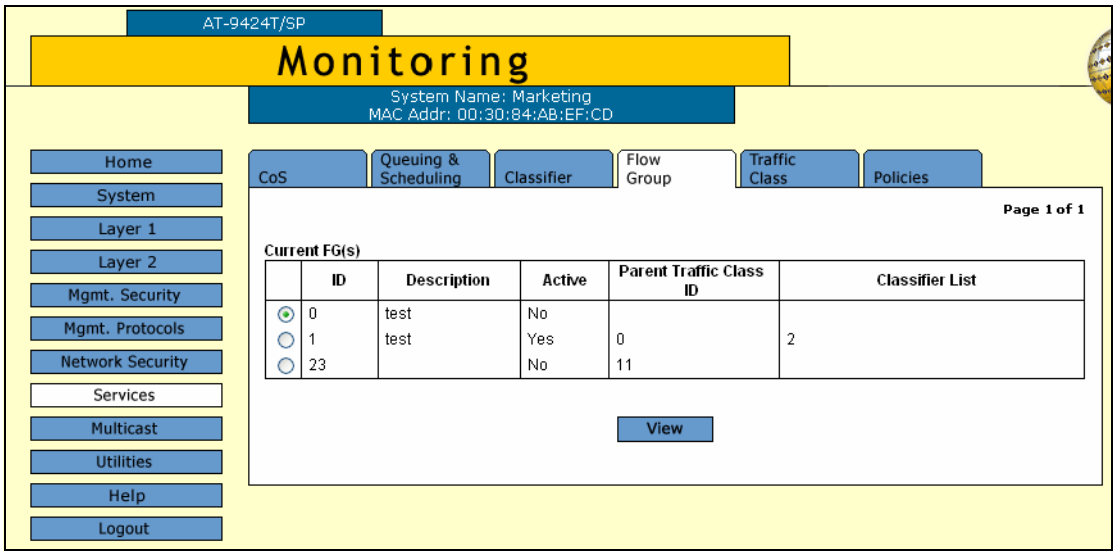

Figure 59. Flow Group Tab (Monitoring)

The Flow Group tab displays the currently configured flow groups in a table that contains the following columns of information:

ID
The ID number of the flow group.

Description
The flow group description.

Active
The active status of the flow group. A flow group is deemed active if it is part of a policy assigned to a switch port. A flow group is considered inactive if it is not assigned to any policies or if the policies have not been assigned to any ports.

Parent Traffic Class ID
The traffic class where the flow group is assigned.

Classifier List
The classifiers of the flow group.

4. To display detailed information about a flow group, select the flow group and click **View**.

   The details of the flow group are displayed in the View Flow Group page. For parameter definitions, refer to "Configuring a Flow Group" on page 166.

5. Click **Close**.

Managing Traffic Classes

This section contains the following procedures:

- ❒ “Configuring a Traffic Class,” next
- ❒ “Modifying a Traffic Class” on page 176
- ❒ “Deleting a Traffic Class” on page 178
- ❒ “Displaying the Traffic Classes” on page 178

Configuring a Traffic Class

To configure a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 60.

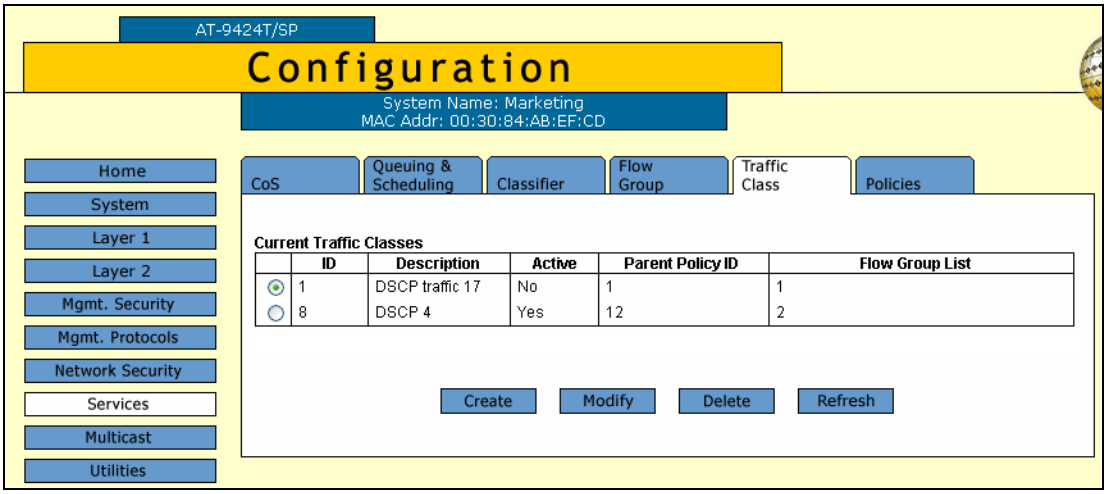

Figure 60. Traffic Class Tab

The columns in the tab are defined here:

ID
The ID of the traffic class.

Description
A description of the traffic class.

Active
Whether this traffic class is active on the switch. An active traffic class is part of a policy assigned to one or more switch ports. An inactive traffic class is not assigned to any policies or to policies that are not assigned to switch ports.

Parent Policy ID
The QoS policies to which the traffic class is assigned.

Flow Group List
The flow groups assigned to this traffic class.

4. To create a new traffic class, click **Create**.

   The Create Traffic Class page is shown in Figure 61.

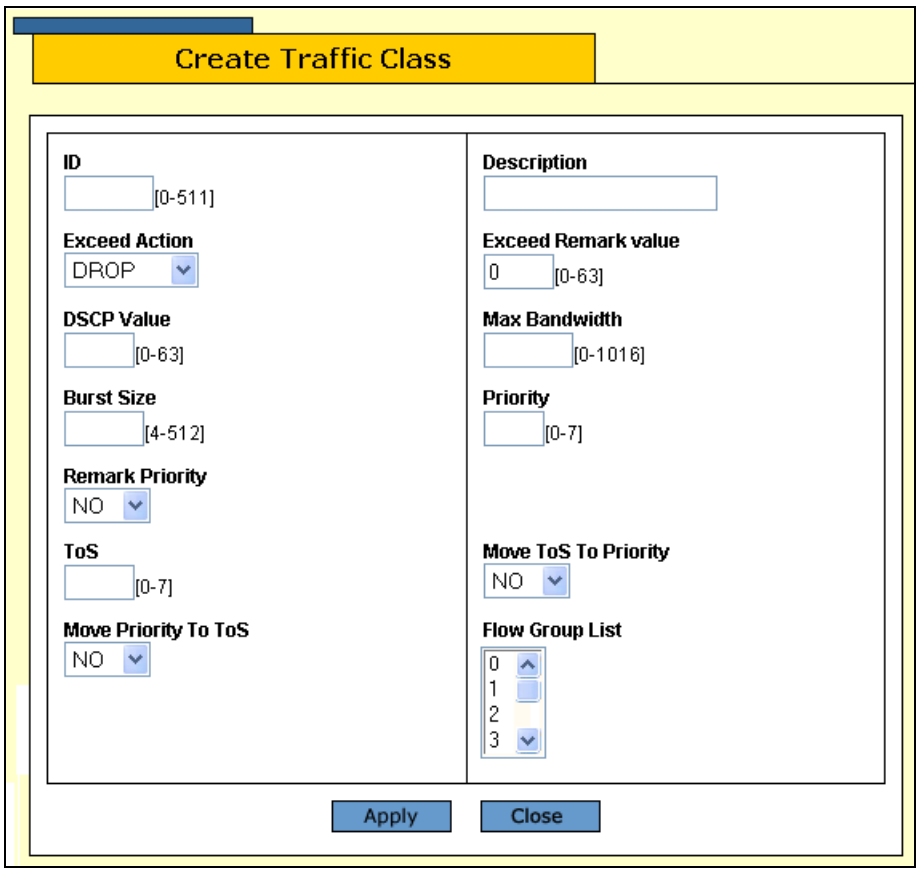

Figure 61. Create Traffic Class Page

5. Configure the following parameters:

   ID
   Specifies an ID number for the traffic class. Each traffic class on the switch must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.

   Description
   Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Action
Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth. There are two possible exceed actions, drop and remark. If drop is selected, traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified in Exceed Remark Value. The default is drop.

Exceed Remark Value
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

DSCP Value
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.

Max Bandwidth
Specifies the maximum bandwidth available to the traffic class. The range is 0 to 1016 Mbps.

This parameter determines the maximum rate at which the ingress port accepts packets belonging to this traffic class before either dropping or remarking occurs, depending on the Exceed Action parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified.

The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).

Note
If this option is set to 0 (zero), all traffic that matches the traffic class is dropped. However, an access control list can be created to match the traffic that is marked for dropping, or a subset of it, and given an action of permit, to override this. This functionality can be used to discard all but a certain type of traffic.

Burst Size
Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. The default is 512 Kbps.

The token bucket is used in situations where you set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded.

Tokens are added to the bucket at the same rate as the traffic class' maximum bandwidth, set with option 6, Max Bandwidth. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at the same rate.

If the amount of traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic is discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added.

Note
To use this parameter you must specify a maximum bandwidth using the Max Bandwidth parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.

Priority
Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of four Class of Service (CoS) queues based on the priority value.

If you want the packets to retain the new value when they exit the switch, change the Remark Priority parameter to Yes.

If you specify a new user priority value here and in Flow Group, the value in Flow Group overwrites the value here.

Remark Priority
Replaces the user priority value in the packets with the new value specified in the Priority parameter, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.

ToS
Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A ToS value can be set at all three levels: flow group, traffic class, and policy. The ToS value in a flow group overrides the value specified at the traffic class or policy level, while the ToS value in a traffic class overrides the value in a policy.

Move ToS to Priority
Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no Does not replace the preexisting 802.1p priority level. This is the default.

Move Priority to ToS
Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no Does not replace the ToS priority field. This is the default.

Flow Group List
Specifies the flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. When you are finished configuring the parameters, click **Apply**.

   The new traffic class is created on the switch.

7. To permanently save your changes, select the **Save Config** menu selection.

Modifying a Traffic Class

This procedure explains how to modify an existing traffic class. If the traffic class to be modified is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can modify the traffic class. You can reassign the ports back to the policy after you have finished modifying the traffic class.

To modify a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 60 on page 172
4. Select the traffic class to be modified and click **Modify**.

   The Modify Traffic Class page is shown in Figure 62.

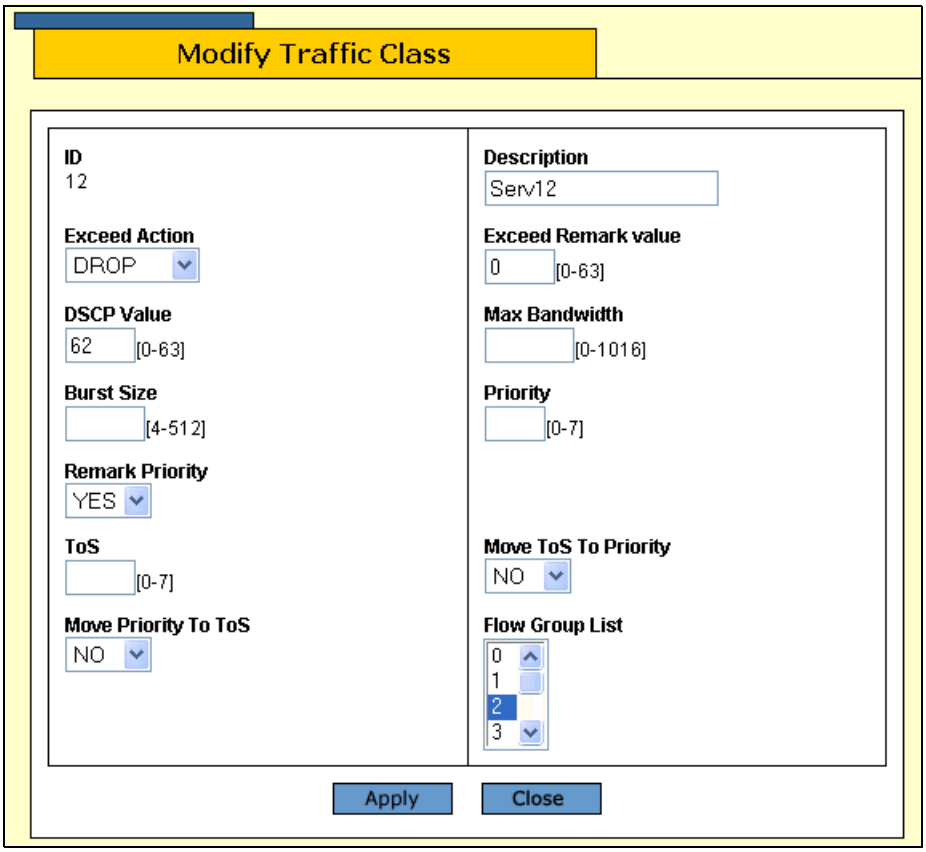

Figure 62. Modify Traffic Class Page

5. Configure the parameters as necessary. For parameter definitions, refer to "Configuring a Traffic Class" on page 172.
6. When you are finished modifying the parameters, click **Apply**.

   The changes are immediately implemented in the traffic class.
7. To permanently save your changes, select the **Save Config** menu selection.

Deleting a Traffic Class

This procedure explains how to delete a traffic class. If the traffic class to be deleted is already part of a QoS policy assigned to one or more switch ports, you must first modify the policy by removing the port assignments before you can delete the traffic class. You can reassign the ports back to the policy after you have deleted the traffic class.

To delete a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 60 on page 172
4. Select the traffic class to be deleted and click **Delete**.

   The traffic class is deleted from the switch.
5. To permanently save your changes, select the **Save Config** menu selection.

Displaying the Traffic Classes

To display the traffic classes, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Services**.
3. Select the **Traffic Class** tab.

   The Traffic Class tab is shown in Figure 63.

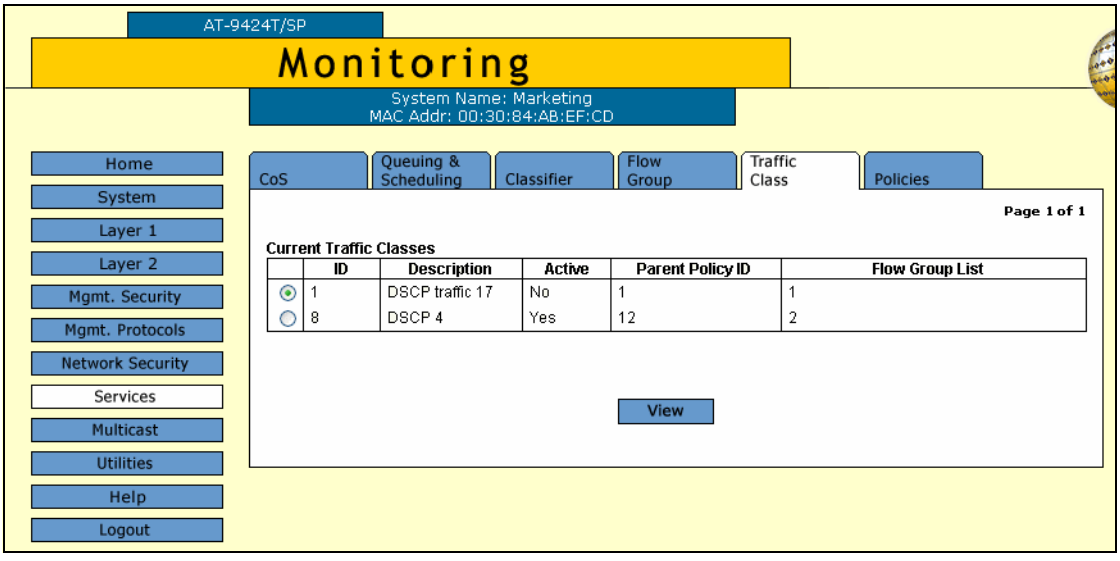

Figure 63. Traffic Class Tab (Monitoring)

The Traffic Class tab displays the currently configured flow groups in a table that contains the following columns of information:

ID
The ID of the traffic class.

Description
A description of the traffic class.

Active
Whether the traffic class is active on the switch. An active traffic class is part of a policy assigned to one or more switch ports. An inactive traffic class is not assigned to any policies or to policies that are not assigned to switch ports.

Parent Policy ID
The QoS policies where the traffic class is assigned.

Flow Group List
The flow groups assigned to this traffic class.

4. To display detailed information about a traffic class, select the traffic class and click **View**.

   The details of the traffic class are displayed in the View Traffic Class page. For parameter definitions, refer to "Configuring a Traffic Class" on page 172.

5. Click **Close**.

Managing Policies

This section contains the following procedures:

- ❒ “Configuring a Policy,” next
- ❒ “Modifying a Policy” on page 183
- ❒ “Deleting a Policy” on page 184
- ❒ “Deleting all Flow Groups, Traffic Classes, and Policies” on page 185
- ❒ “Displaying Policies” on page 185

Configuring a Policy

To configure a policy, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 64.

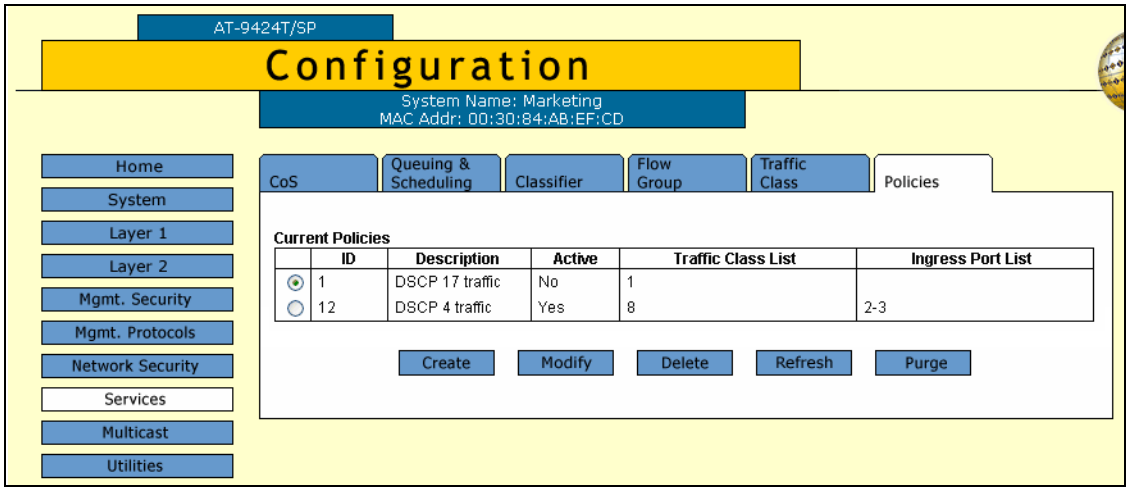

Figure 64. Policies Tab (Configuration)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID
The ID of the policy.

Description
A description of the policy.

Active
Whether this policy is active on the switch. An active policy is assigned to one or more switch ports. An inactive policy is not assigned to any switch ports.

Traffic Class List
The traffic classes assigned to the policy.

Ingress Port List
The ingress ports to which the policy is assigned.

4. Click **Create**.

   The Create Policy page opens, as shown in Figure 65.

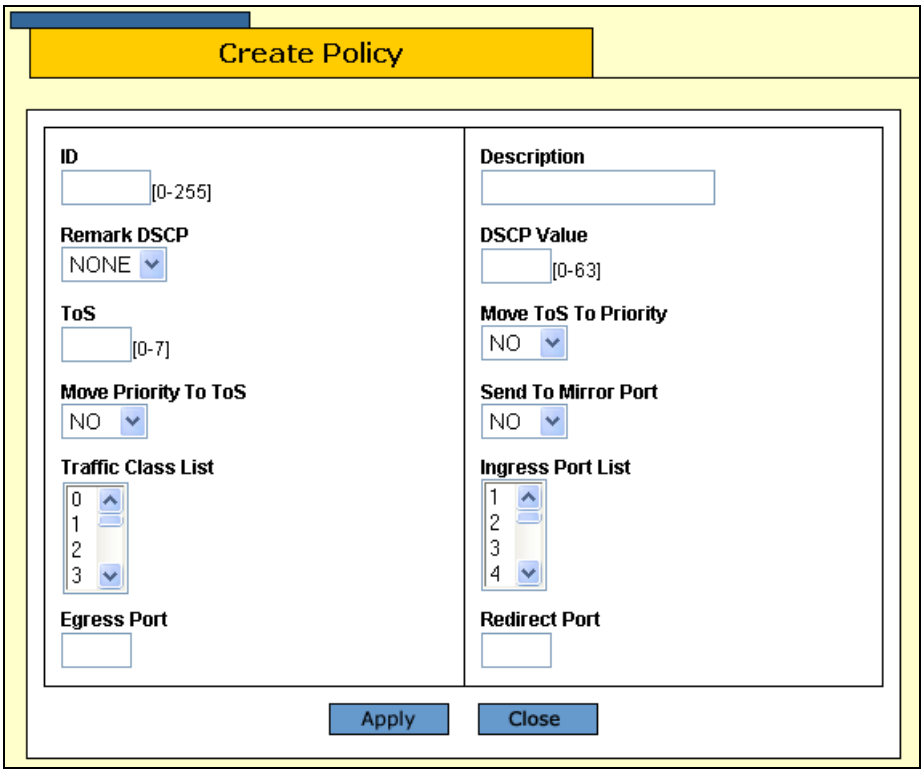

Figure 65. Create Policy Page

5. Configure the following parameters as necessary:

   ID
   Specifies an ID number for the policy. Every policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.

   Description
   Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

Remark DSCP
Specifies whether the ingress DSCP value is overwritten. Select one of the following options from the list:

None - Disables this function.

All - All packets are remarked.

DSCP Value
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.

ToS
Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A ToS value can be set at all three levels: flow group, traffic class, and policy. The ToS value in a flow group overrides the value specified at the traffic class or policy level, while the ToS value in a traffic class overrides the value in a policy.

Move ToS to Priority
Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no Does not replace the preexisting 802.1p priority level. This is the default.

Move Priority to ToS
Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no Does not replace the ToS priority field. This is the default.

Send to Mirror Port
Copies the traffic that meets the criteria of the policy's classifiers to a destination mirror port. Options are:

Yes Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror. For instructions, refer to "Creating a Port Mirror" on page 96.

No Does not copy the traffic to a destination mirror port. This is the default.

Traffic Class List
Specifies the traffic class to be assigned to the policy. The traffic class must already exist. A policy can have more than one traffic class. To select more than one traffic class, hold down the Ctrl key when making your selections.

Ingress Port List
Specifies the ingress port to which the policy is to be assigned. A policy can be assigned to more than one ingress port. To select more than one port, hold down the Ctrl key when you make your selections. A port can be an ingress port of only one policy at a time.

Egress Port
Specifies the egress port to which the policy is to be assigned. You can enter only one egress port.

A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.

Redirect Port
Specifies a port to where the traffic is to be redirected. Traffic that matches the defined traffic flow is redirected to the specified port. You can specify only one port.

6. When you are finished configuring the parameters, click **Apply**.

   If the new policy was assigned ports, it is now active on the designated ports.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Policy

To modify a policy, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 64 on page 180.

4. Select the policy to be modified from the list and click **Modify**.

The Modify Policy page is shown in Figure 66.

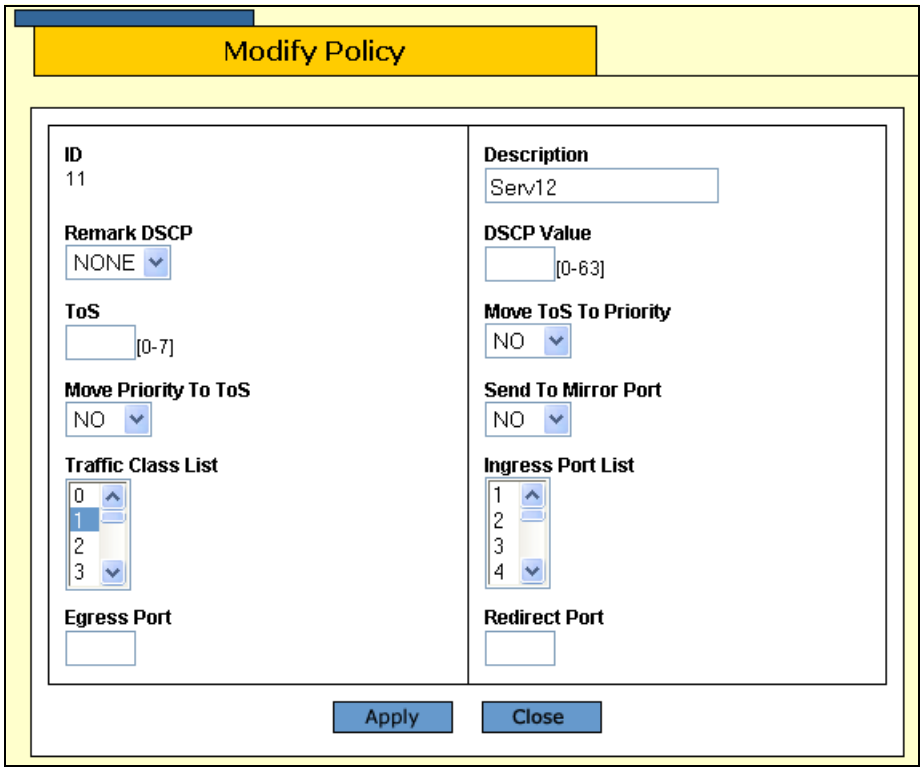

Figure 66. Modify Policy Page

5. Modify the parameters as needed. For parameter definitions, refer to “Configuring a Policy” on page 180.
6. When you are finished configuring the parameters, click **Apply**.

   The changes are immediately implemented in the policy.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Policy

To delete a policy, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 64 on page 180.
4. Select a policy from the list and click **Delete**. You can only delete one policy at a time.

   The policy is deleted from the switch.

5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting all Flow Groups, Traffic Classes, and Policies

To delete all flow groups, traffic classes, and policies from the switch, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Services** option.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 64 on page 180.
4. Click **Purge** to delete all flow groups, traffic classes, and policies from the switch.

   The switch deletes all flow groups, traffic classes, and policies.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying Policies

To display the policies, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Services**.
3. Select the **Policies** tab.

   The Policies tab is shown in Figure 67.

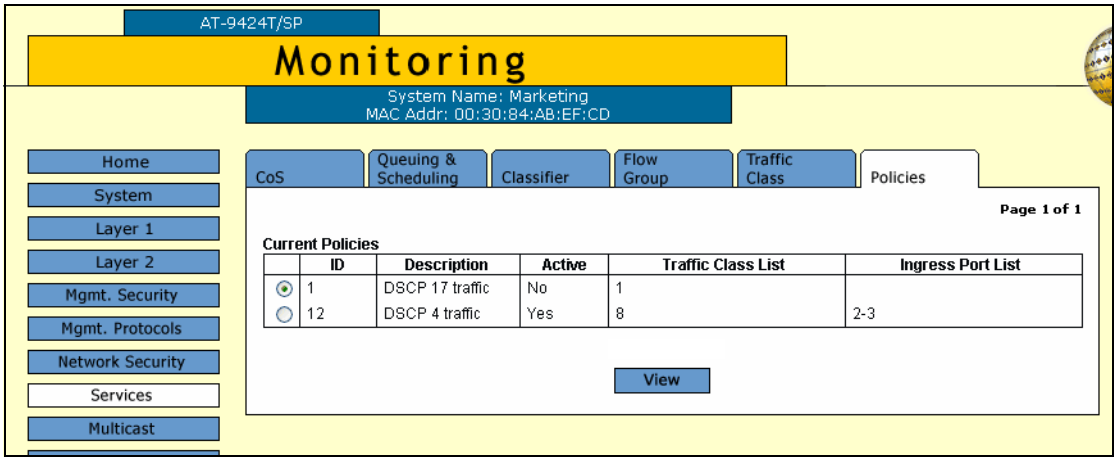

Figure 67. Policies Tab (Monitoring)

The Policies tab displays the existing policies in a table with the following columns of information:

ID
The ID of the policy.

Description
A description of the policy.

Active
Whether this policy is active on the switch. An active policy is assigned to one or more switch ports. An inactive policy is not assigned to any switch ports.

Traffic Class List
The traffic classes of the policy.

Ingress Port List
The ingress ports of the policy.

4. To view the details of a specific policy, select the policy and click View.

   The settings of the policy are displayed in the View Policy page. For parameter definitions, refer to “Configuring a Policy” on page 180.

5. Click **Close**.

Chapter 15

Denial of Service Defenses

This chapter contains instructions on how to configure the Denial of Service defense feature on the switch. The sections include:

- ❒ “Configuring Denial of Service Defense” on page 188
- ❒ “Displaying the DoS Settings” on page 191

Configuring Denial of Service Defense

To configure the ports on the switch for a Denial of Service attack defense, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **DoS** tab.

   The DoS tab is shown in Figure 68.

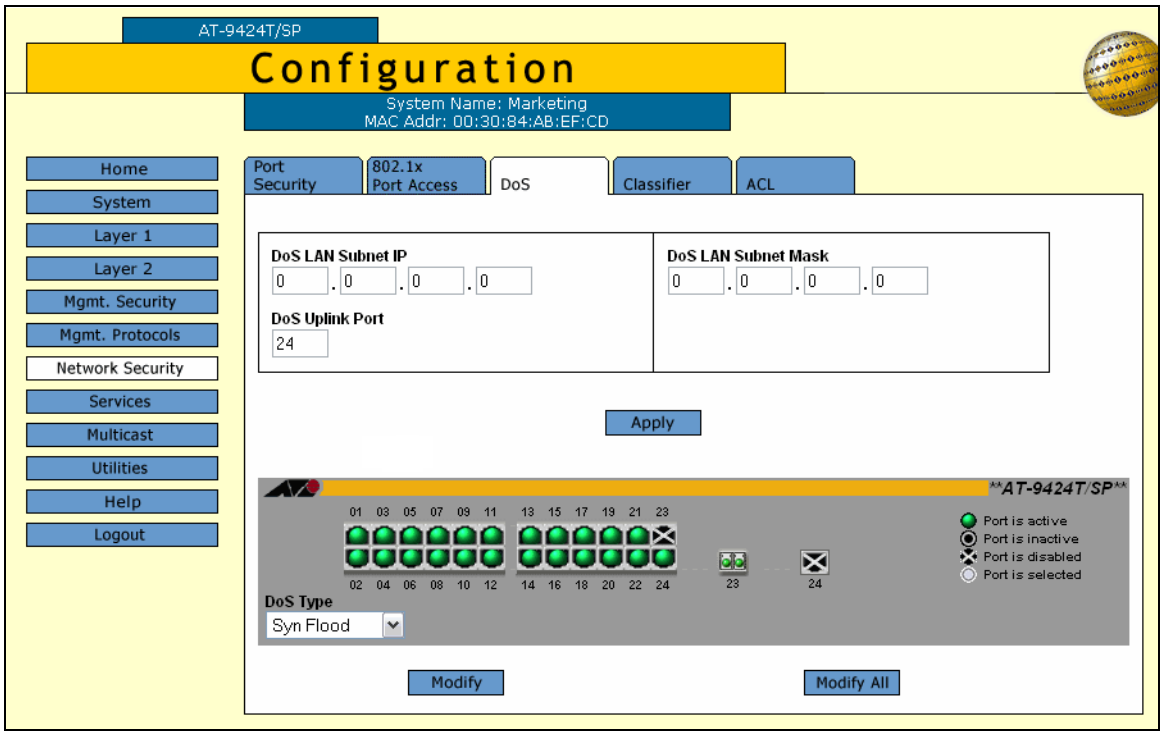

Figure 68. DoS Tab (Configuration)

4. If you are implementing the SMURF or Land defense, you must provide an IP address and mask for your LAN. To do this, complete the following procedure. Otherwise, skip ahead to Step 5.

   a. In the DoS LAN Subnet IP field, enter the IP address of one of the devices connected to the switch, preferably the lowest IP address.

   b. In the DoS Subnet Mask field, enter the LAN's mask. enter the mask. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to

149.11.11.50. The mask would be 0.0.0.63.

c. If you are activating the Land defense, in the DoS Uplink Port field enter the number of the port connected to the device (e.g., DSL router) that leads outside your network. You can specify only one uplink port.

5. Click the ports in the switch image where a defense mechanism is to be enabled or disabled.

6. Using the DoS Type list, select the type of denial of service attack to be enabled or disabled on the ports. The possible selections are:

   - Syn Flood attack
   - Smurf attack
   - Land attack
   - Tear drop attack
   - Ping of death attack
   - IP Options

7. Click **Modify**. To configure all the ports, click **Modify All**.

   The DoS Configuration for Ports page opens. The page shown in Figure 69 is for IP Options.

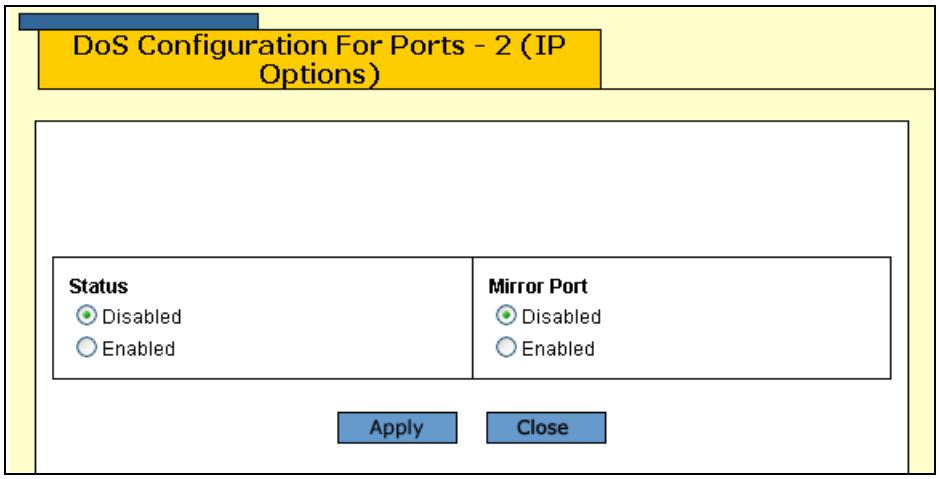

Figure 69. DoS Configuration for Ports Page

8. Configure the following parameters as necessary:

   Status
   Click Enable or Disable to enable or disable DoS on the selected ports.

   Mirror Port
   This option applies to the Land, Tear Drop, Ping of Death, and IP Options. Enabling this option mirrors the traffic examined by a defense mechanism to another port on the switch. To use this feature, you must activate port mirroring on the switch and specify a destination mirror port, as explained in “Creating a Port Mirror” on page 96.

9. Click **Apply**.

   The defense is immediately activated on the ports.

10. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the DoS Settings

To display the DoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Network Security**.
3. Select the **DoS** tab.

   The DoS tab is shown in Figure 70.

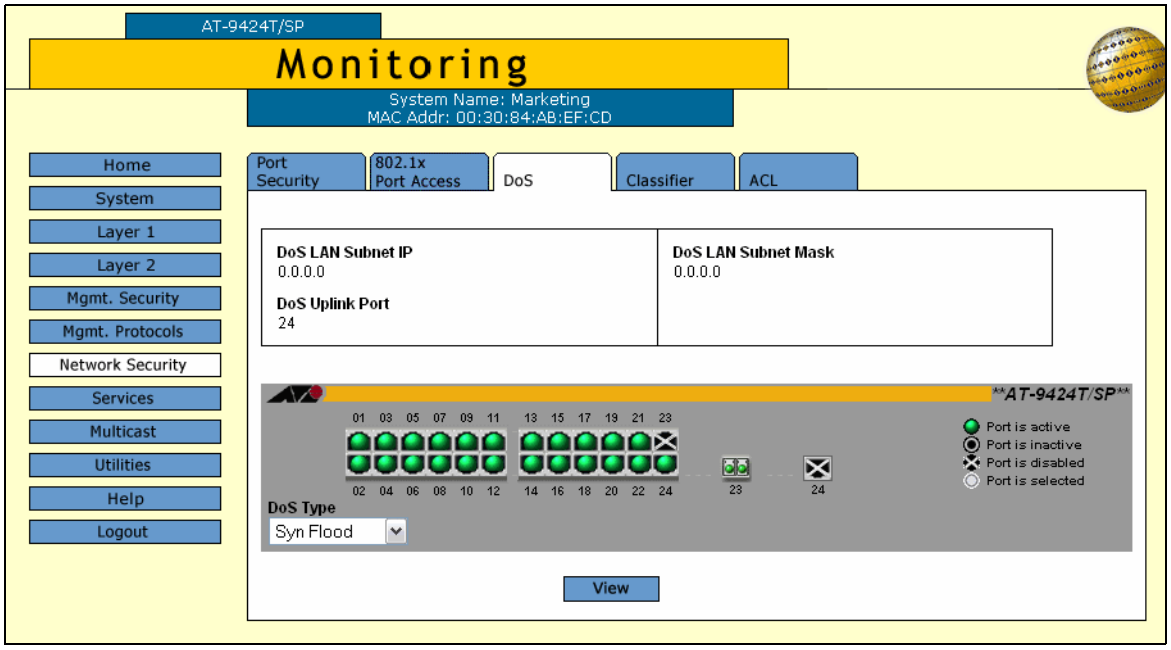

Figure 70. DoS Tab (Monitoring)

4. Click the port whose DoS settings are to be displayed. You can select more than one port at a time.
5. Using the DoS Type list, select the type of Denial of Service defense whose settings are to be displayed.
6. Click **View**.

The DoS Monitor for Port page opens, as shown in Figure 71.

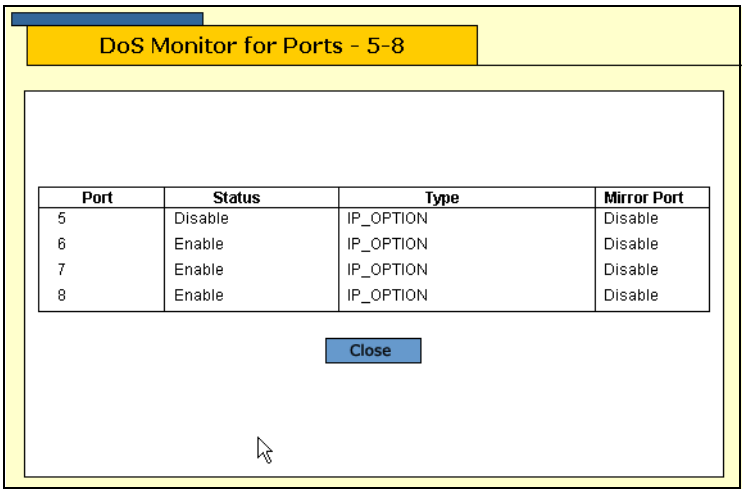

Figure 71. DoS Monitor for Ports Page

The page displays a table that contains the following columns of information:

Port
The port number.

Status
Whether DoS is enabled or disabled on the port.

Type
The type of DoS prevention.

Mirror Port
Whether the examined traffic is copied to a mirror port.

Chapter 16
IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. The sections in the chapter include:

- ❒ “Configuring IGMP Snooping” on page 194
- ❒ “Displaying a List of Host Nodes” on page 197
- ❒ “Displaying a List of Multicast Routers” on page 199

Configuring IGMP Snooping

To configure IGMP snooping, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Multicast** option.

   The Multicast page is displayed with the **IGMP** tab selected by default, as shown in Figure 72.

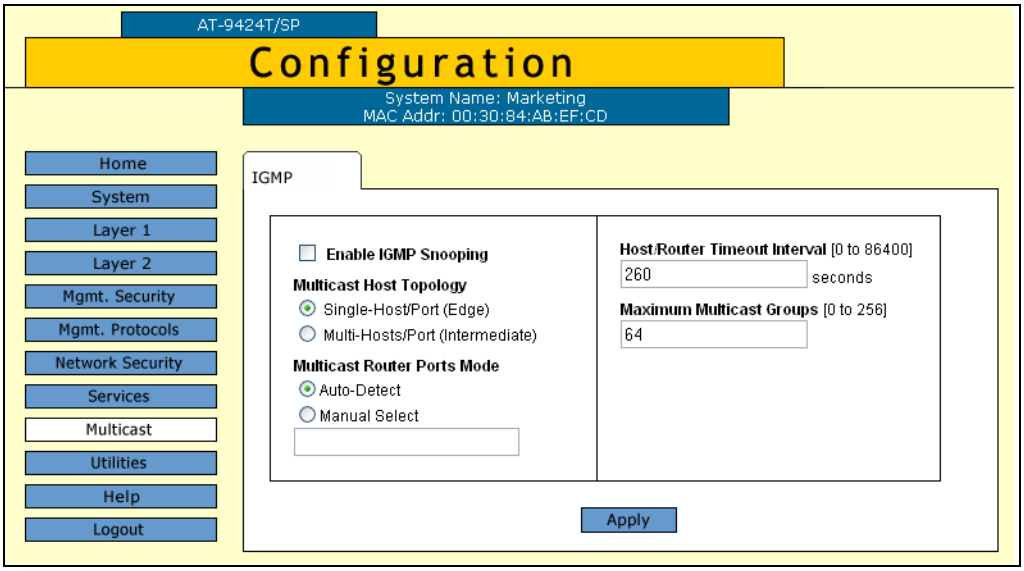

Figure 72. IGMP Tab (Configuration)

3. Configure the following parameters as necessary.

   Enable IGMP Snooping Status
   Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP snooping is enabled.

   Multicast Host Topology
   Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

   The Single-Host/Port (Edge) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Multi-Host/Port (Intermediate) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port (Intermediate) selection.

Multicast Router Ports Mode
Specifies whether the router ports are determined automatically or if you enter them manually. If you want the switch to determine the ports automatically, select Auto-Detect, which is the default. To enter them yourself, click Manual Select and enter the ports in the field.

Host/Router Timeout Interval
Specifies the time period in seconds at which the switch determines that a host node is inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds. If you set the timeout to zero (0), the timer never times out, and the timeout interval is essentially disabled.

This parameter also controls the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

The actual timeout may be ten seconds less that the specified value. For example, a setting of 25 seconds can result in the switch classifying a host node or multicast router as inactive after just 15 seconds. A setting of 10 seconds or less can result in the immediate timeout of an inactive host node or router.

Maximum Multicast Groups
Specifies the maximum number of IGMP multicast groups the switch can learn. This parameter is useful with networks that contain a large number of multicast groups. The range is 0 to 255 groups. The default is 64 multicast groups.

Note
The combined number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

4. Click **Apply**.

   Changes to the IGMP snooping parameters are immediately implemented on the switch.

5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying a List of Host Nodes

You can use the AT-S63 Management Software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes.

To view host nodes, perform the following procedure:

1. From the Home page, select **Monitoring**.

2. From the Monitoring menu, select the **Multicast** option.

   The Multicast page is displayed with the IGMP tab as shown in Figure 73.

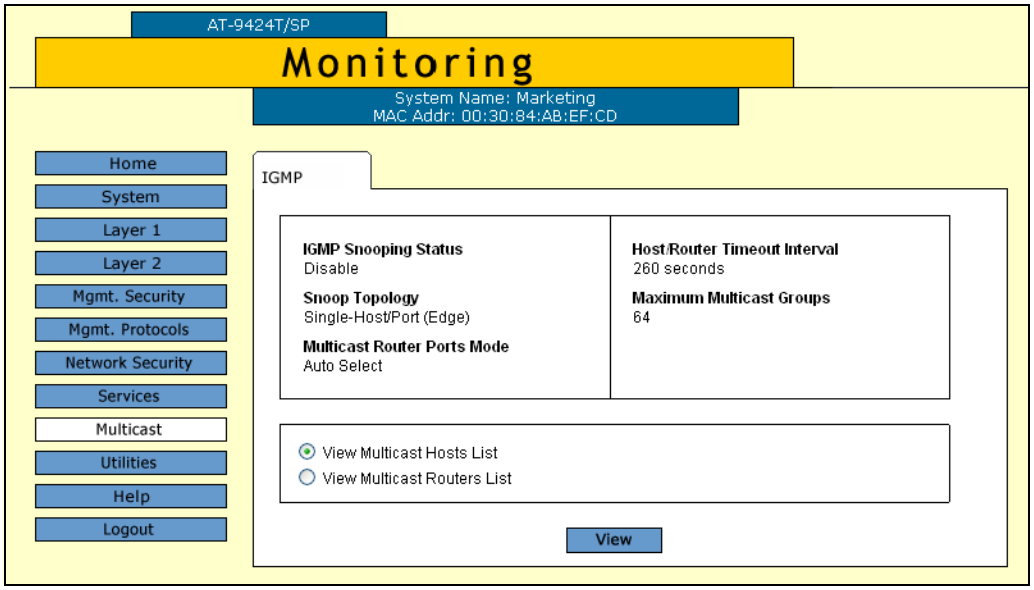

Figure 73. IGMP Tab (Monitoring)

   For definitions of the parameters in the tab, refer to "Configuring IGMP Snooping" on page 194.

3. To view the multicast addresses and the host nodes, click **View Multicast Hosts List** and then click **View**.

   The View Multicast Hosts List page is displayed. The page contains the following columns of information:

   Multicast Group
   The multicast address of the group.

VLAN ID
The VID of the VLAN where the port is an untagged member.

Member Port/Trunk ID
The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.

Host IP
The IP address of the host node connected to the port.

Version
The version of IGMP used by the host.

Exp. Time
The number of seconds remaining before the host is timed out if no further IGMP reports are received from it.

Displaying a List of Multicast Routers

To view multicast routers, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Multicast** option.

   The Multicast page is displayed with the IGMP tab as shown in Figure 73 on page 197.
3. To view the multicast routers, click **View Multicast Router List** and then click **View**.

   The View Multicast Routers List is shown in Figure 74.

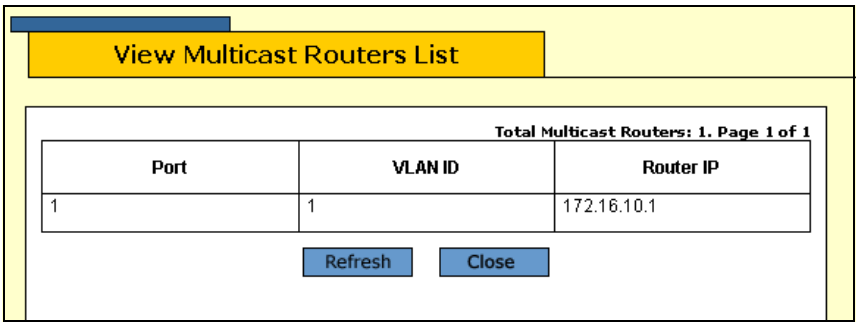

Figure 74. View Multicast Routers List Page

The View Multicast Routers List page displays a table that contains the following columns of information:

Port
The port on the switch where the multicast router is connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the port on the router.

Section III
SNMPv3

This section has the following chapter:

- Chapter 17, “SNMPv3” on page 203

Chapter 17
SNMPv3

This chapter provides the following procedures for configuring SNMPv3 parameters using a web browser management session:

- ❒ “Configuring the SNMPv3 Protocol” on page 204
- ❒ “Enabling or Disabling SNMP Management” on page 205
- ❒ “Configuring the SNMPv3 User Table” on page 208
- ❒ “Configuring the SNMPv3 View Table” on page 216
- ❒ “Configuring the SNMPv3 Access Table” on page 222
- ❒ “Configuring the SNMPv3 SecurityToGroup Table” on page 229
- ❒ “Configuring the SNMPv3 Notify Table” on page 235
- ❒ “Configuring the SNMPv3 Target Address Table” on page 240
- ❒ “Configuring the SNMPv3 Target Parameters Table” on page 247
- ❒ “Configuring the SNMPv3 Community Table” on page 254
- ❒ “Displaying SNMPv3 Tables” on page 260

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to first enable SNMP access on the switch. Then you configure the SNMPv3 tables. See the following procedures:

- ❒ “Enabling or Disabling SNMP Management” on page 205
- ❒ “Configuring the SNMPv3 User Table” on page 208
- ❒ “Configuring the SNMPv3 View Table” on page 216
- ❒ “Configuring the SNMPv3 Access Table” on page 222
- ❒ “Configuring the SNMPv3 SecurityToGroup Table” on page 229
- ❒ “Configuring the SNMPv3 Notify Table” on page 235
- ❒ “Configuring the SNMPv3 Target Address Table” on page 240
- ❒ “Configuring the SNMPv3 Target Parameters Table” on page 247
- ❒ “Configuring the SNMPv3 Community Table” on page 254

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesis does not recommend this configuration.

Enabling or Disabling SNMP Management

In order to allow an SNMP manager or host to access the switch you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a login attempt from an unauthenticated user, you need to enable authentication failure traps. This section provides a procedure to accomplish both of these tasks.

To enable SNMP access and authentication failure traps, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 158 on page 388.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 75.

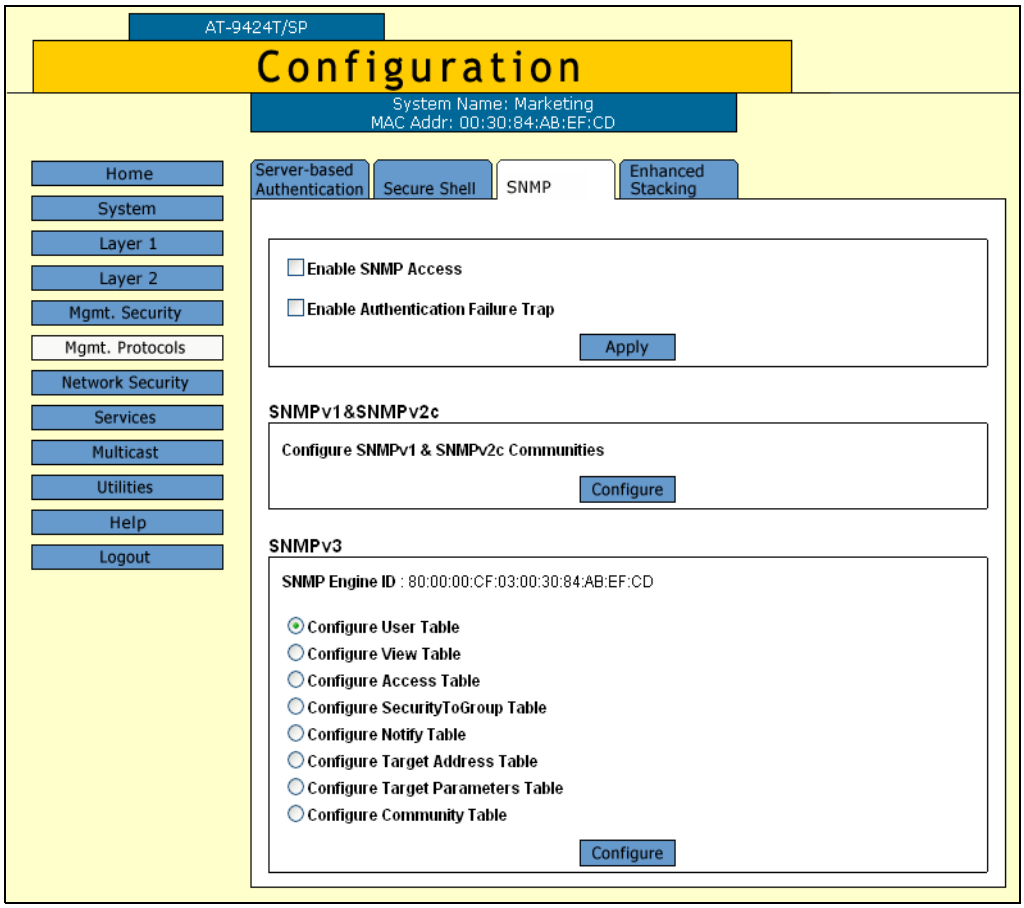

Figure 75. SNMP Tab (Configuration)

4. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

   Use this parameter to enable the switch to be remotely managed with an SNMP application program.

   Note
   If the Enable SNMP Access check box is not checked, the switch cannot be managed through SNMP. This is the default.

5. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.

6. Click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 User Table

You can create, delete, and modify an SNMPv3 User Table entry. See the following procedures:

- “Creating a User Table Entry” on page 208
- “Deleting a User Table Entry” on page 211
- “Modifying a User Table Entry” on page 212

For reference information about the SNMPv3 User Table, see Chapter 21, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 75 on page 206.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 76.

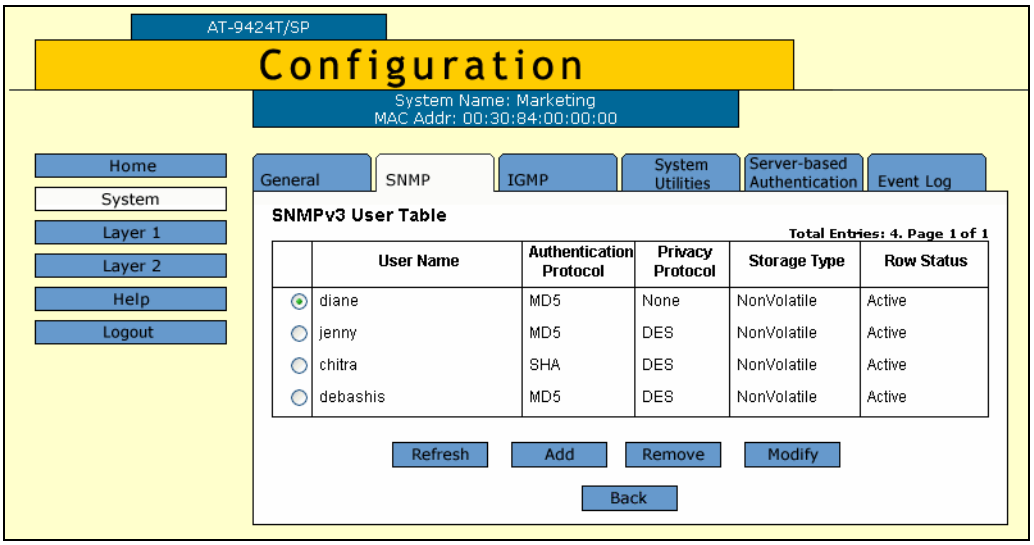

Figure 76. SNMPv3 User Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 User page is shown in Figure 77.

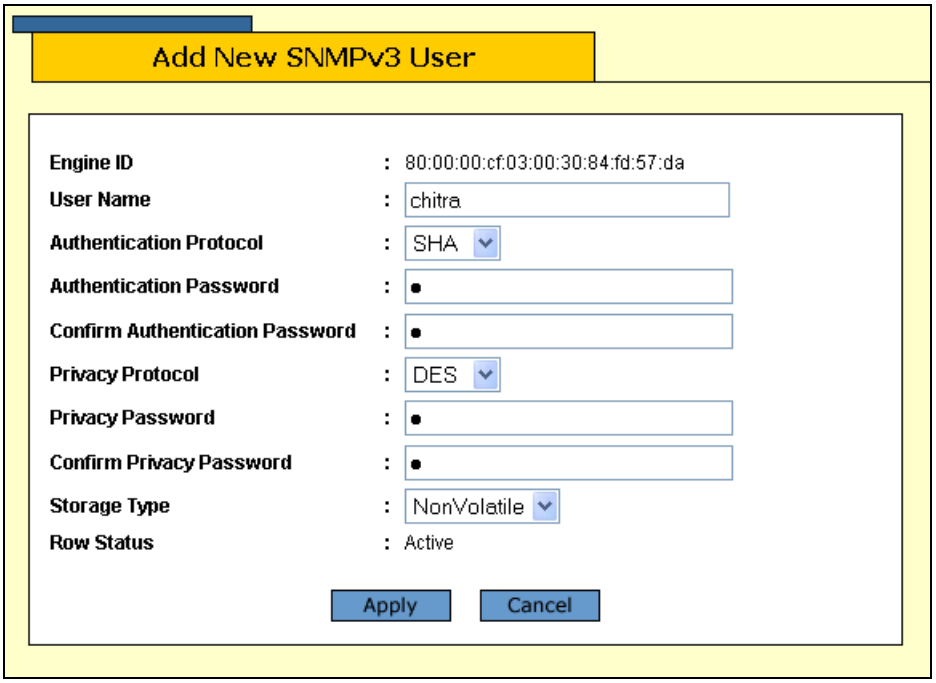

Figure 77. Add New SNMPv3 User Page

5. In the User Name field, enter a name, or logon id, that consists of up to 32 alphanumeric characters

6. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

   Note
   You may want to assign NONE to a super user.

7. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

8. In the Confirm Authentication Password field, re-enter the authentication password.

   Note
   If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

   Note
   You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

9. In the Privacy Protocol field, enter one of the following options:

   DES
   Select this value to make the DES privacy (or encryption) protocol the

privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None
Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

10. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

11. In the Confirm Privacy Password field, re-enter the privacy password.

12. In the Storage Type field, enter one of the following storage options for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the User Table. After making changes to an User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the User Table. After making changes to an User Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.

14. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a User Table Entry

To delete an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

   The SNMPv3 User Table tab is shown in Figure 76 on page 209.

4. Click the button next to the User Table entry to be deleted and click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a User Table Entry

To modify an entry SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

   The SNMPv3 User Table tab is shown in Figure 76 on page 209.

4. Click the button next to the SNMPv3 user to be changed and then click **Modify**.

The Modify SNMPv3 User page is shown in Figure 78.

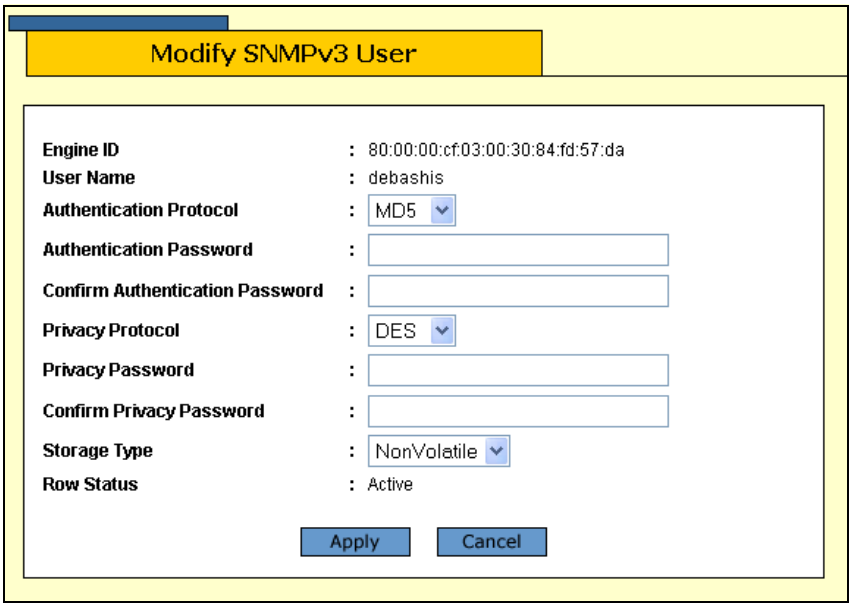

Figure 78. Modify SNMPv3 User Page

5. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

   Select one of the following:

   MD5
   This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

   SHA
   This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

   None
   This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note
You may want to assign NONE to a super user.

6. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.

7. In the Confirm Authentication Password field, re-enter the authentication password.

Note
If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note
You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

8. In the Privacy Protocol field, enter one of the following options:

   DES
   Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

   None
   Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

9. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.

10. In the Confirm Privacy Password field, re-enter the privacy password.

11. In the Storage Type field, enter one of the following storage options for this User Table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table

entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 User Table.
13. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 View Table

You can create, delete, and modify an SNMPv3 View Table entry. See the following procedures:

- “Creating a View Table Entry” on page 216
- “Deleting a View Table Entry” on page 219
- “Modifying a View Table Entry” on page 219

For reference information about the SNMPv3 View Table, see Chapter 21, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a View Table Entry

To create an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 79.

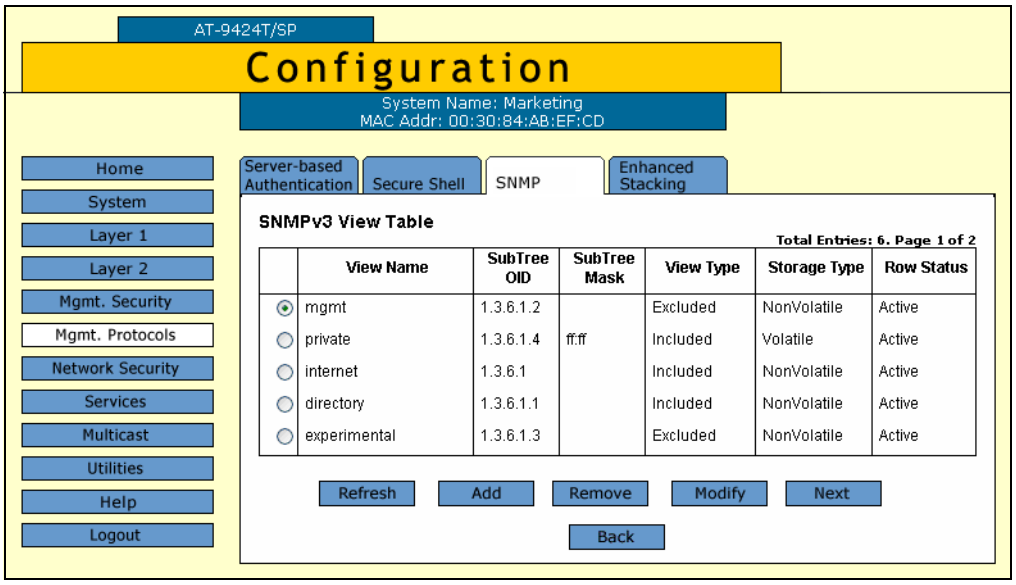

Figure 79. SNMPv3 View Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 View page is shown in Figure 80.

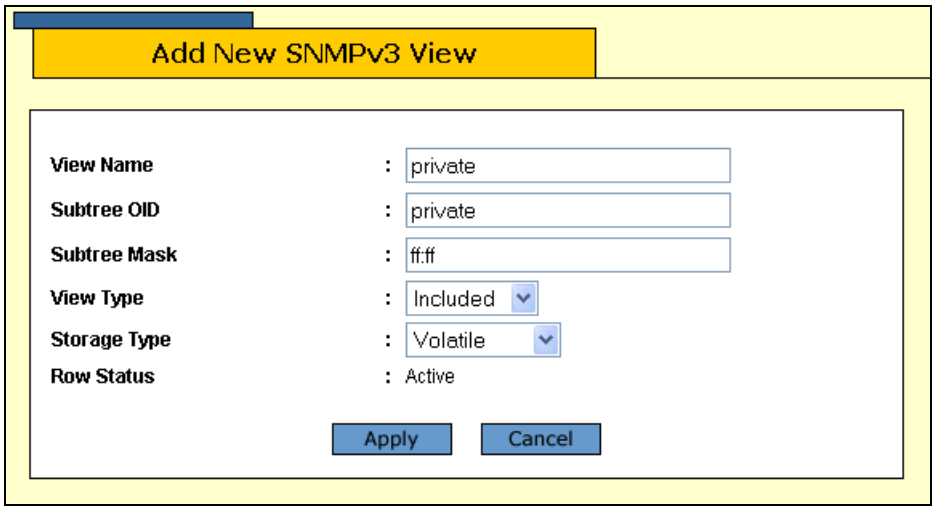

Figure 80. Add New SNMPv3 View Page

5. In the View Name field, enter a descriptive name for this view.

   Assign a name that reflects the subtree OID, for example, "internet." Enter a unique name of up to 32 alphanumeric characters.

Note
The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use the default value for an SNMPv3 View Table entry.

6. In the Subtree OID field, enter a subtree that this view will or will not be permitted to display.

   You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:

   ```
   1.3.6.1.2.1.6
   ```

   The text format is for TCP/IP is:

   ```
   tcp
   ```

7. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

   This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

   The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user’s view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

   ```
   1.3.6.1.2.1.2.2.1.0.3
   ```

   To restrict the user’s view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

   ```
   ff:bf
   ```

8. In the View Type field, enter one of the following view types:

   Included
   Enter this value to permit the user to see the subtree specified above.

   Excluded
   Enter this value to not permit the user to see the subtree specified above.

9. In the Storage Type field, enter a storage type for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the View Table. After making changes to a View Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile
Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 View Table.
11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a View Table Entry

To delete an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure**.

   The SNMPv3 View Table tab is shown in Figure 79 on page 217.

4. Click the button next to the View Table entry to be deleted and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.
6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a View Table Entry

To modify an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to Configure View Table and then click **Configure** at the bottom of the tab.

   The SNMPv3 View Table tab is shown in Figure 79 on page 217.

4. Click the button next to the SNMPv3 View Table entry to be changed and then click **Modify**.

   The Modify SNMPv3 View page is shown in Figure 81.

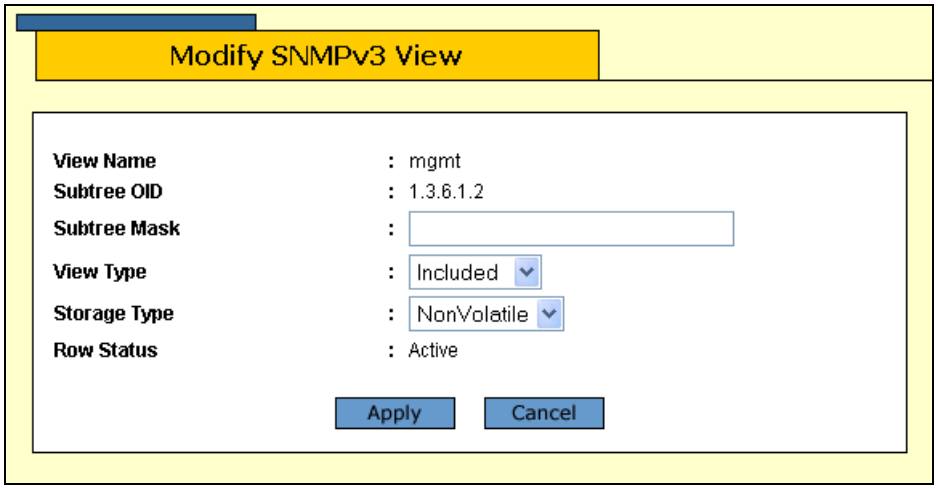

Figure 81. Modify SNMPv3 View Page

5. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

   This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

   The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

   ```
   1.3.6.1.2.1.2.2.1.0.3
   ```

   To restrict the user's view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

   ```
   ff:bf
   ```

6. In the View Type field, enter one of the following view types:

Included
Enter this value to permit the View Name to see the subtree specified above.

Excluded
Enter this value to not permit the View Name to see the subtree specified above.

7. In the Storage Type field, enter a storage type for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

8. Click **Apply**.

9. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 Access Table

You can create, delete, and modify an SNMPv3 Access Table entry. See the following procedures:

- “Creating an Access Table” on page 222
- “Deleting an Access Table Entry” on page 225
- “Modifying an Access Table Entry” on page 226

For information about the SNMPv3 Access Table, see Chapter 21, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating an Access Table

To create an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 82.

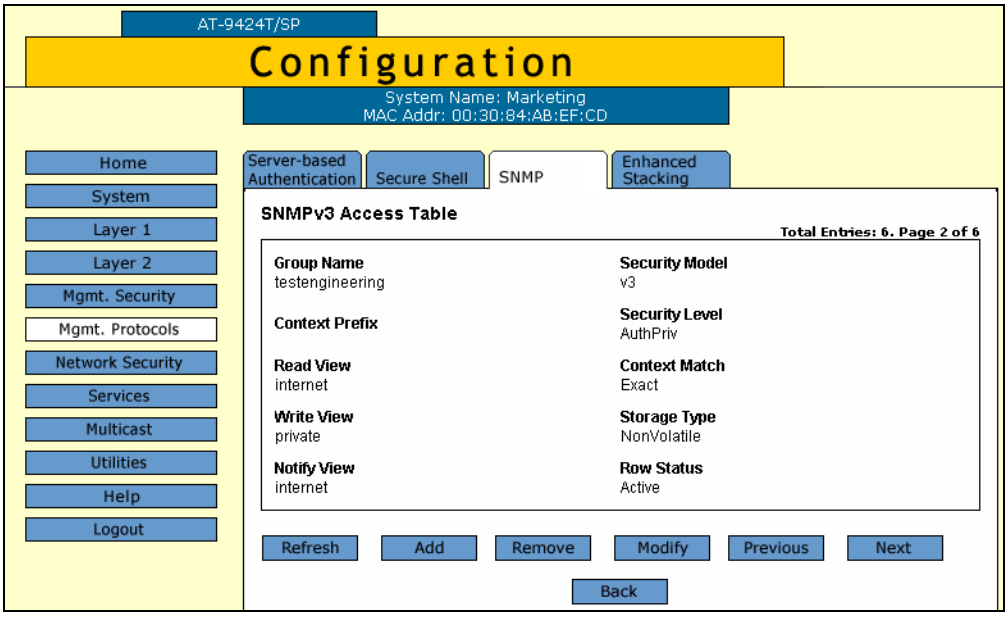

Figure 82. SNMPv3 Access Table Tab (Configuration)

4. To create an SNMPv3 Access Table entry, click **Add**.

   The Add New SNMPv3 Access page is shown in Figure 83.

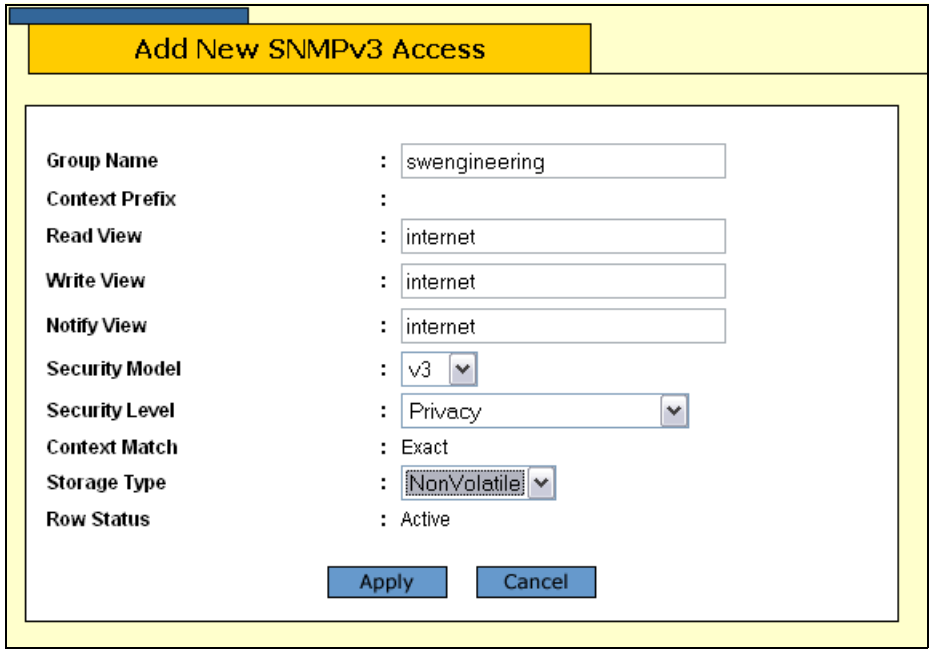

Figure 83. Add New SNMPv3 Access Page

5. In the Group Name field, enter a descriptive name of the group.

   The Group Name can consist of up to 32 alphanumeric characters.

   You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, a unique group name makes it easier for you to tell the groups apart.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

   Note
   The Context Prefix field is a read only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

9. In the Security Model field, enter an SNMP protocol.

   Select one of the following SNMP protocols as the Security Model for this Group Name.

   v1
   Select this value to associate the Group Name with the SNMPv1 protocol.

   v2c
   Select this value to associate the Group Name with the SNMPv2c protocol.

   v3
   Select this value to associate the Group Name with the SNMPv3 protocol.

10. In the Security Level field, enter a security level.

    Select one of the following security levels:

    No Authentication/Privacy
    This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This option provides the least security.

    Note
    If you have selected SNMPv1 or SNMPv2c, N-NoAuthNoPriv is the only security level you can select.

    Authentication
    This option permits an authentication protocol, but not a privacy

protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Note
The Context Match field is a read only field. The Context Match field is always set to Exact.

11. In the Storage Type field, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

12. Click **Apply**.

13. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting an Access Table Entry

To delete an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 82 on page 222.

4. Click **Next** or **Previous** to display the Access Table entry to be deleted.

5. Click **Remove**.

   A warning message is displayed. Click OK to remove the Access Table entry.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Access Table tab is shown in Figure 82 on page 222.

4. Click **Next** or **Previous** to display the Access Table entry to be changed.

5. Click **Modify**.

   The Modify SNMPv3 Access page is shown in Figure 84.

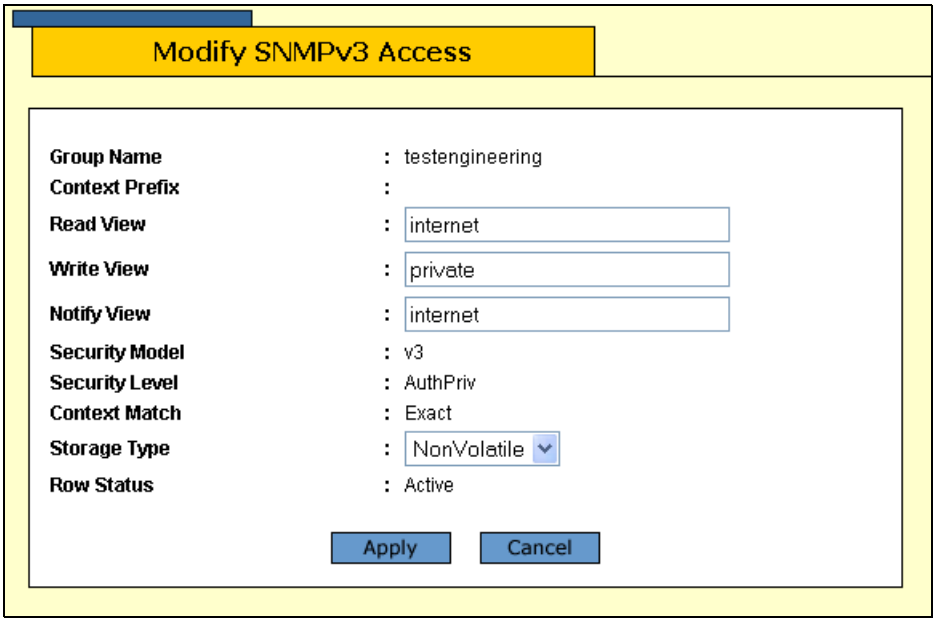

Figure 84. Modify SNMPv3 Access Page

Note
The Context Prefix field is a read-only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the View Table.

   This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

Note
The Context Match field is a read only field. The Context Match field is always set to Exact.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the Access Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Access Table.

11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 SecurityToGroup Table

You can create, delete, and modify an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- "Creating a SecurityToGroup Table Entry" on page 229
- "Deleting a SecurityToGroup Table Entry" on page 232
- "Modifying a SecurityToGroup Table Entry" on page 232

For reference information about the SNMPv3 SecuritytoGroup Table, see Chapter 21, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 85.

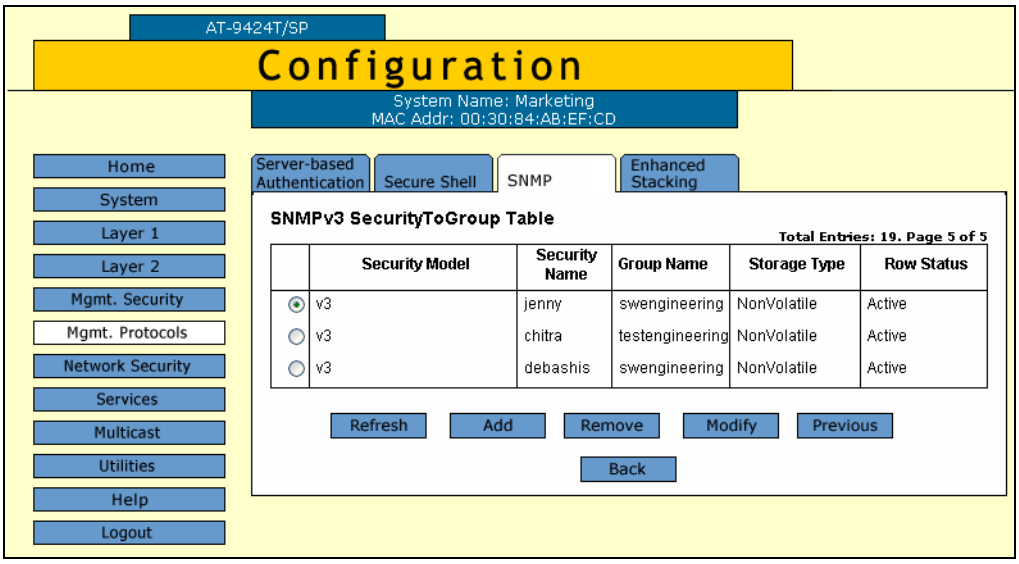

Figure 85. SNMPv3 SecurityToGroup Table Tab (Configuration)

4. To create an SNMPv3 SecurityToGroup Table entry, click **Add**.

   The Add New SNMPv3 SecurityToGroup page is shown in Figure 86.

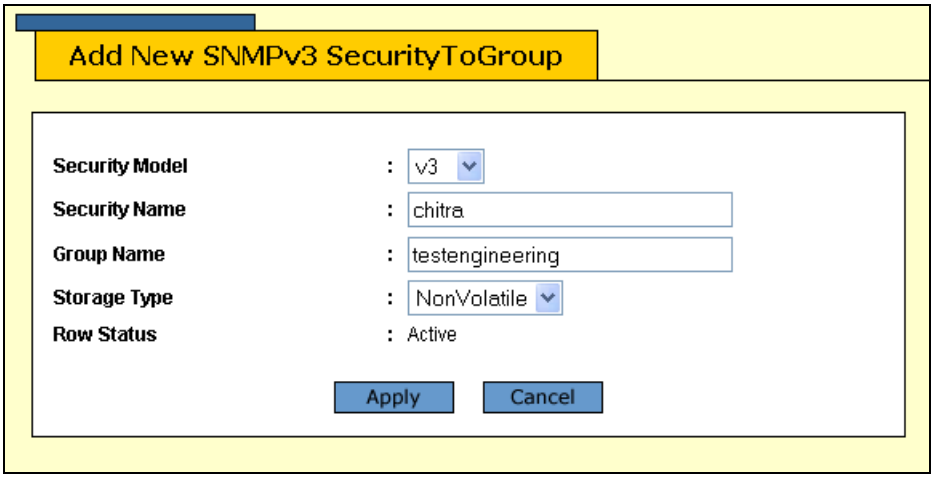

Figure 86. Add New SNMPv3 SecurityToGroup Page

5. In the Security Model field, select the SNMP protocol that was configured for this User Name.

   Choose from the following:

   v1
   Select this value to associate the Group Name with the SNMPv1 protocol.

v2c
Select this value to associate the Group Name with the SNMPv2c protocol.

v3
Select this value to associate the Group Name with the SNMPv3 protocol.

6. In the Security Name field, enter the User Name to be associated with a group.

   Enter a User Name that you configured in "Creating a User Table Entry" on page 208.

7. In the Group Name field, enter a Group Name that you configured in the Access Table.

   See "Creating an Access Table" on page 222.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

9. Click **Apply**.

10. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a SecurityToGroup Table Entry

To delete an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table**, and then click **Configure** at the bottom of the tab.

   The SNMPv3 SecurityToGroup Table tab is shown in Figure 85 on page 230.

4. Click the button next to the SecurityToGroup Table entry to be deleted and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a SecurityToGroup Table Entry

To modify an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 SecurityToGroup Table tab is shown in Figure 85 on page 230.

4. Click the button next to the SecurityToGroup Table entry to be changed, and then click **Modify**.

   The Modify SNMPv3 SecurityToGroup page is shown in Figure 87.

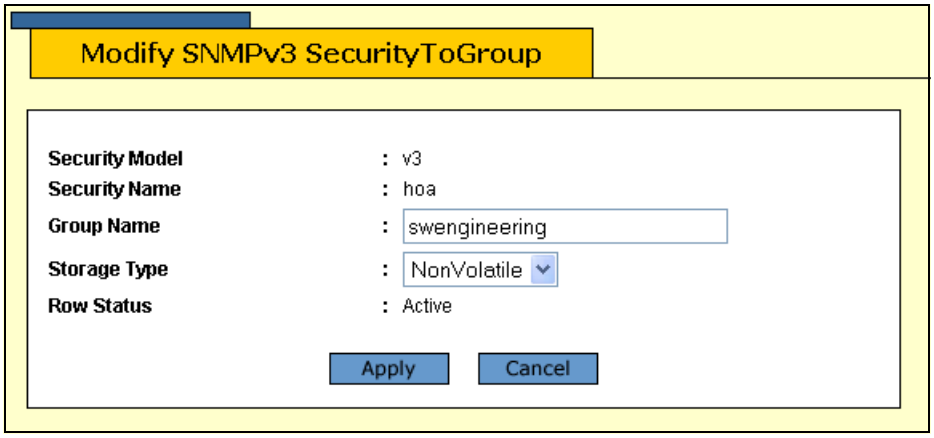

Figure 87. Modify SNMPv3 SecurityToGroup Page

5. In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

   See "Creating an Access Table" on page 222.

   There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

   - defaultV1GroupReadOnly
   - defaultV1GroupReadWrite
   - defaultV2cGroupReadOnly
   - defaultV2cGroupReadWrite

6. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

7. Click **Apply** to update the SNMPv3 SecurityToGroup Table.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 Notify Table

You can create, delete, and modify an SNMPv3 Notify Table entry. See the following procedures:

- "Creating a Notify Table Entry" on page 235
- "Deleting a Notify Table Entry" on page 237
- "Modifying a Notify Table Entry" on page 238

For reference information about the SNMPv3 Notify Table, see Chapter 21, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 88.

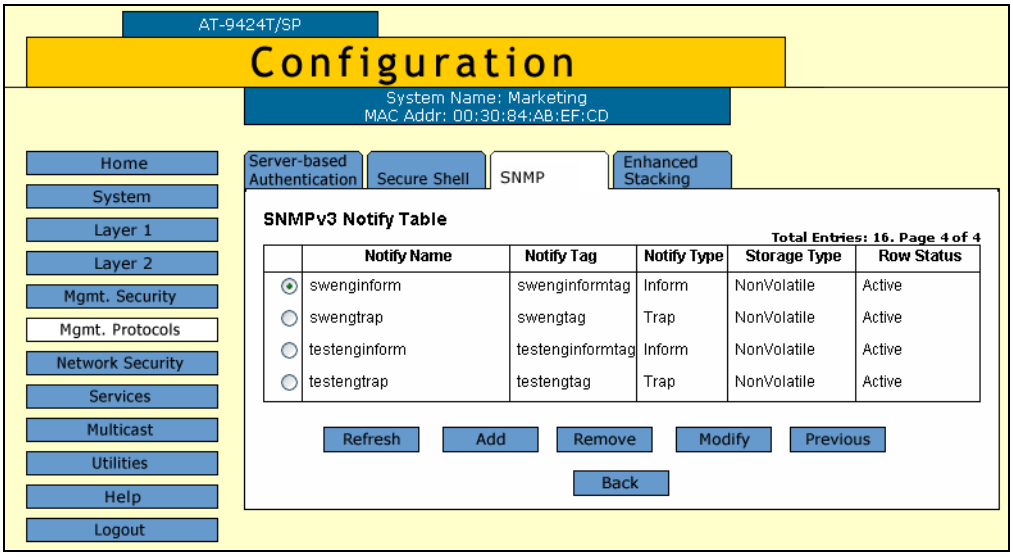

Figure 88. SNMPv3 Notify Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Notify page is shown in Figure 89.

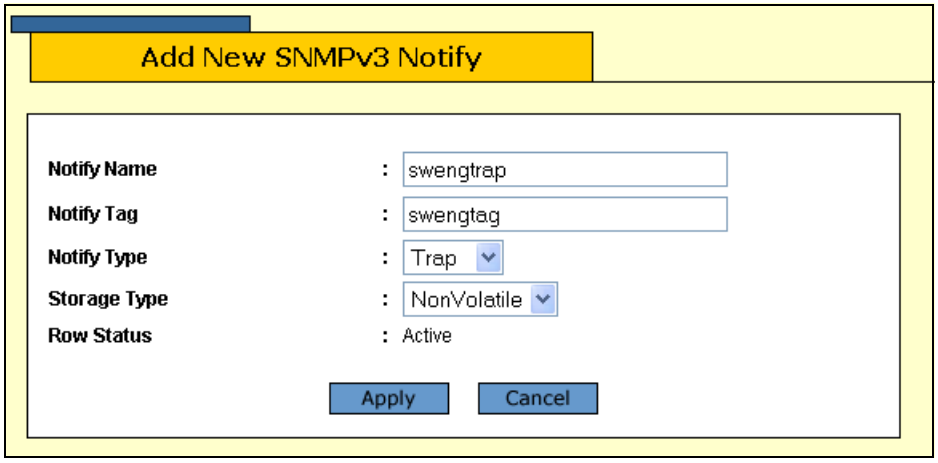

Figure 89. Add New SNMPv3 Notify Page

5. In the Notify Name field, enter the name associated with this trap message.

   Enter a descriptive name of up to 32 alphanumeric characters. For example, you might want to define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.

6. In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

7. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.

10. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Notify Table Entry

To delete an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

   The SNMPv3 Notify Table tab is shown in Figure 88 on page 236.

4. Click the button next to the Notify Table entry to be deleted, and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Notify Table Entry

To modify an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to Configure Notify Table, and then click **Configure** at the bottom of the tab.

   The SNMPv3 Notify Table tab is shown in Figure 88 on page 236.

4. Click the button next to the table entry to be changed and then click **Modify**.

   The Modify SNMPv3 Notify page is shown in Figure 90.

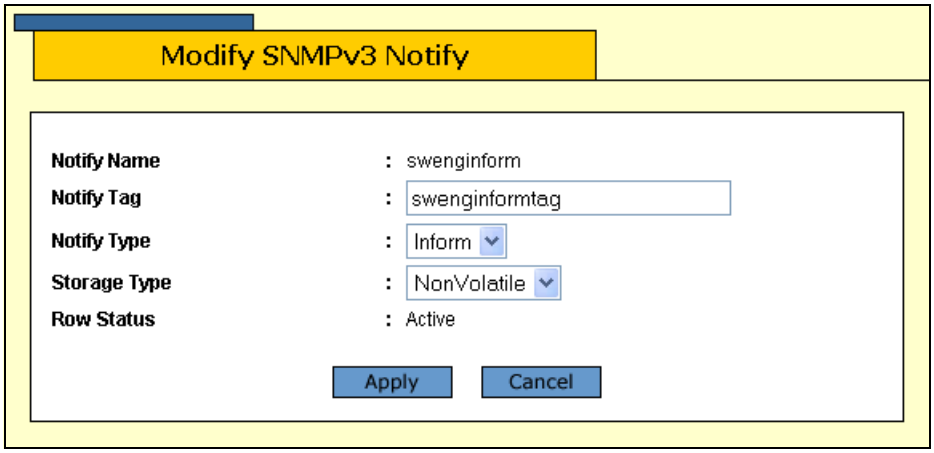

Figure 90. Modify SNMPv3 Notify Page

5. In the Notify Tag field, enter a description name of the Notify Tag.

   Enter a name of up to 32 alphanumeric characters.

6. In the Notify Type field, enter one of the following message types:

   Trap
   Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the host.

   Inform
   Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

7. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 Notify Table.

9. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 Target Address Table

You can create, delete, and modify an SNMPv3 Target Address Table entry. See the following procedures:

- “Creating a Target Address Table Entry” on page 240
- “Deleting a Target Address Table Entry” on page 243
- “Modifying Target Address Table Entry” on page 244

For reference information about the SNMPv3 Target Address Table, see Chapter 21, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 91.

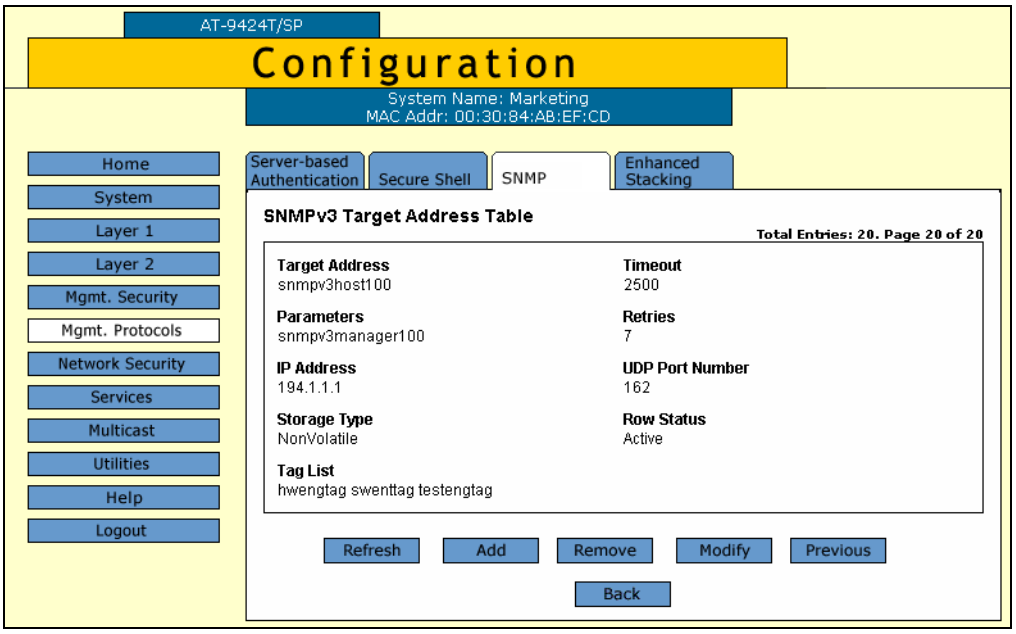

Figure 91. SNMPv3 Target Address Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Target Address page is shown in Figure 92.

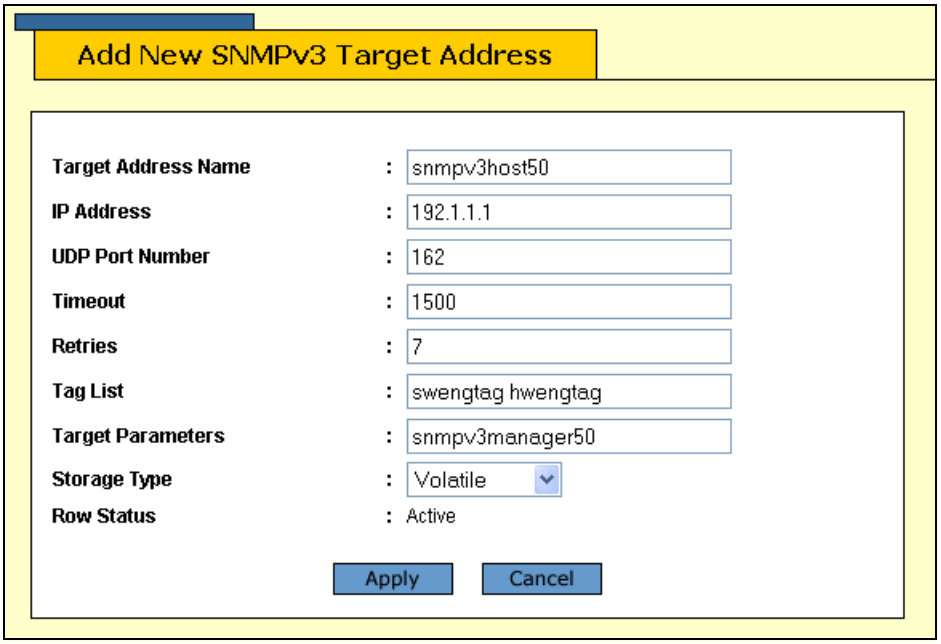

Figure 92. Add New SNMPv3 Target Address Page

5. In the Target Address Name field, enter the name of the SNMP manager, or host, that manages the SNMP activity on your switch.

You can enter a name of up to 32 alphanumeric characters.

6. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address:
   XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

   You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

   When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured in a SNMPv3 Notify Table with the Notify Tag parameter.

    See “Creating a Notify Table Entry” on page 235. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

11. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the SNMPv3 Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile
Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Address Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Target Address Table Entry

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Address Table tab is shown in Figure 91 on page 241.

4. Click **Next** or **Previous** to display the SNMPv3 Target Address Table entry to be deleted.
5. Click **Remove**.

   A warning message is displayed.

6. Click **OK**.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Address Table tab is shown in Figure 91 on page 241.

4. Click **Next** or **Previous** to display the Target Address Table entry to be changed.

5. Click **Modify**.

   The Modify SNMPv3 Target Address page is shown Figure 93.

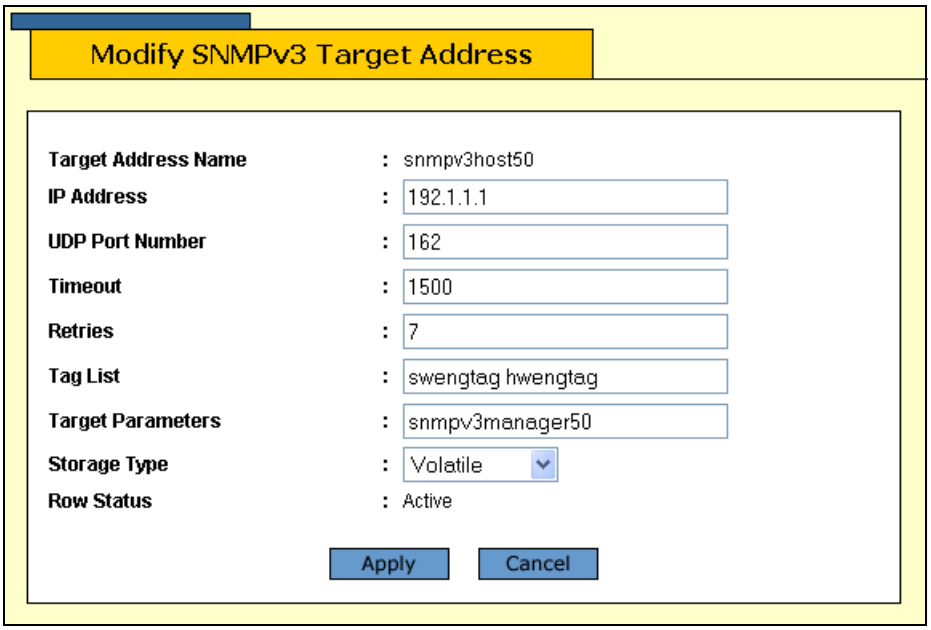

Figure 93. Modify SNMPv3 Target Address Page

6. In the IP Address field, enter the IP address of the host.

   Use the following format for an IP address:
   XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

   You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

   When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

   When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured with the Notify Tag parameter in a Notify Table entry.

    See "Creating a Notify Table Entry" on page 235. Enter a Tag List of up to 256-alphanumeric characters. Use a space to separate entries, for example:

    ```
    hwengtag swengtag testengtag
    ```

11. In the Target Parameters field, enter a Target Parameters name.

    This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to an Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

13. Click **Apply** to update the SNMPv3 Target Address Table.

14. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 Target Parameters Table

You can create, delete, and modify an SNMPv3 Target Parameters Table entry. See the following procedures:

- "Creating a Target Address Table Entry" on page 240
- "Deleting a Target Address Table Entry" on page 243
- "Modifying Target Address Table Entry" on page 244

For reference information about the SNMPv3 Target Parameters Table, see Chapter 21, "SNMPv3" in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 94.

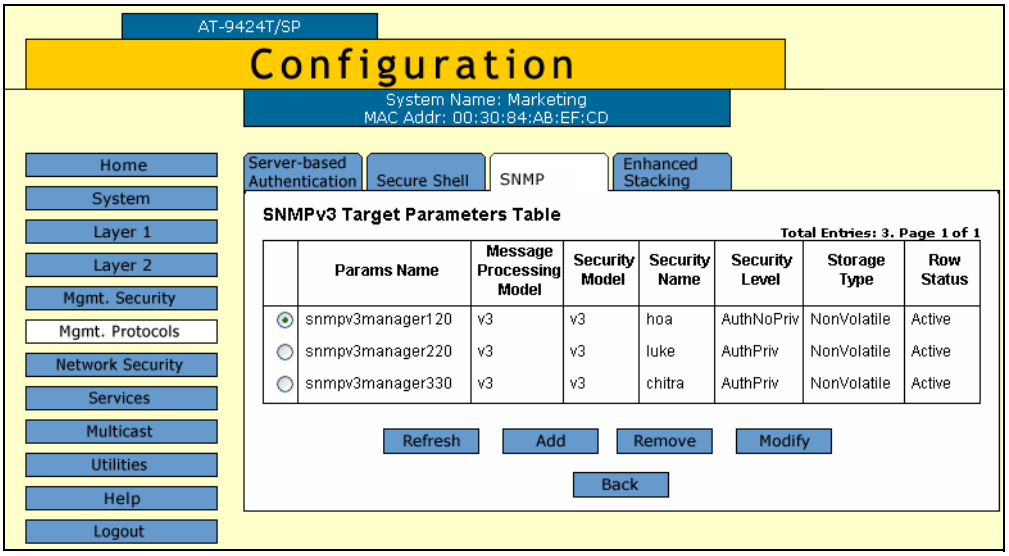

Figure 94. SNMPv3 Target Parameters Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Target Parameter page is shown in Figure 95.

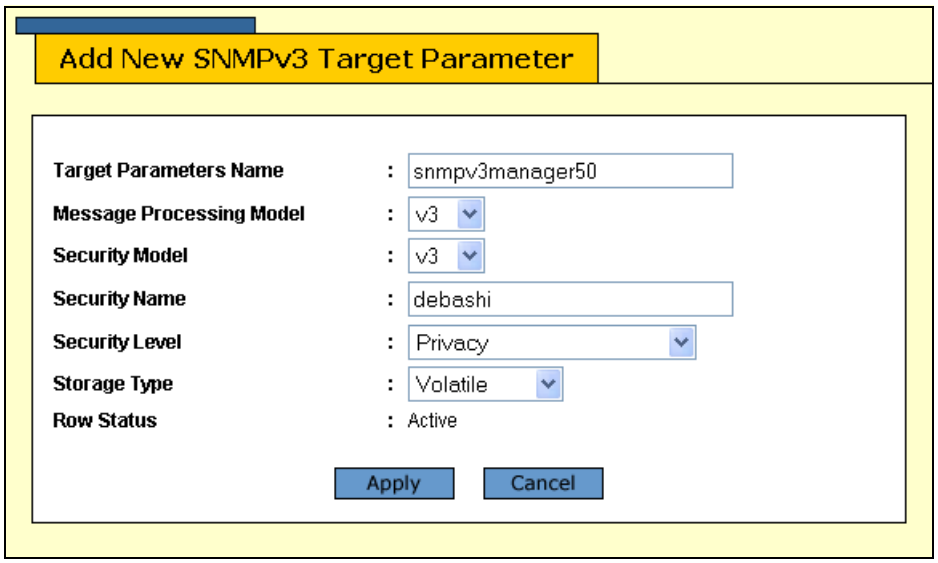

Figure 95. Add New SNMPv3 Target Parameters Page

5. In the Target Parameters Name field, enter a name of the SNMP manager or host.

   Enter a value of up to 32 alphanumeric characters.

> **Note**
> Enter a value for the Message Processing Model parameter only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the Message Processing Model is automatically assigned to SNMPv3.

6. In the Message Processing Model field, enter a Security Model that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

7. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1
Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c
Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3
Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

8. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See "Creating a User Table Entry" on page 208.

9. In the Security Level field, select one of the following Security Levels:

   Note
   The value you configure for the Security Level must match the value configured for the User Name in the User Table Menu. See "Creating a User Table Entry" on page 208.

   No Authentication/Privacy
   This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

   Note
   If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

   Authentication
   This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

   Privacy
   This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

10. In the Storage Type parameter, select one of the following storage types for this table entry:

    Volatile
    Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

    NonVolatile
    Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

    Note
    The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Target Parameters Table.

12. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a Target Parameters Table Entry

To delete an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 94 on page 247.

4. Click the button next to the Target Parameters Table entry to be deleted and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a Target Parameters Table Entry

To modify an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Target Parameters Table tab is shown in Figure 94 on page 247.

4. Click the button next to the Target Parameters Table entry to be changed, and then click **Modify**.

   The Modify SNMPv3 Target Parameter page is shown in Figure 96 on page 251.

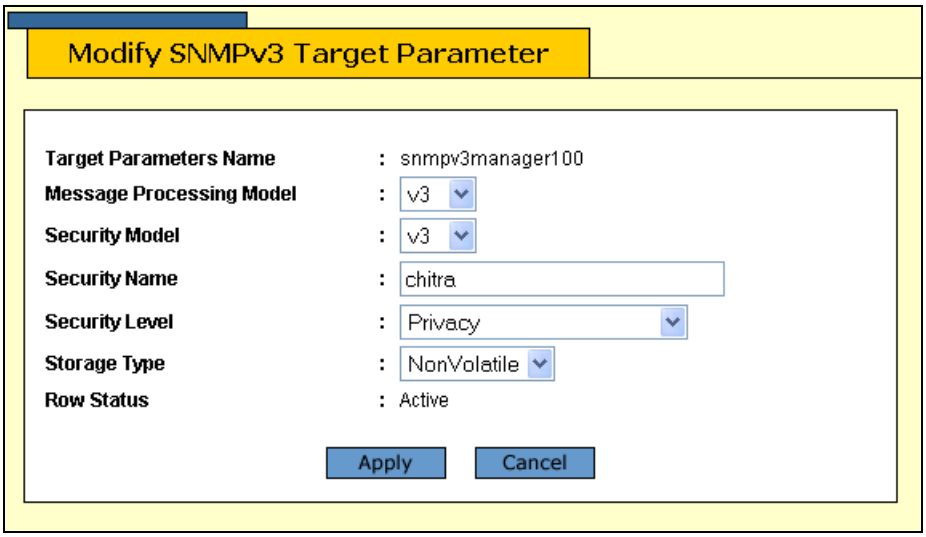

Figure 96. Modify SNMPv3 Target Parameter Page

Note
Enter a value for the Message Processing Model field only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the switch automatically assigns the Message Processing Model to SNMPv3.

5. In the Message Processing Model field, enter a Security Model that is used to process messages.

   Select one of the following SNMP protocols:

   v1
   Select this value to process messages with the SNMPv1 protocol.

   v2c
   Select this value to process messages with the SNMPv2c protocol.

   v3
   Select this value to process messages with the SNMPv3 protocol.

6. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

   v1
   Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

   v2c
   Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

   v3
   Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

7. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

   See “Creating a User Table Entry” on page 208.

8. In the Security Level field, select one of the following Security Levels:

   Note
   The value you configure for the Security Level must match the value configured for the User Name in the SNMPv3 User Table Menu. See “Creating a User Table Entry” on page 208.

   No Authentication/Privacy
   This option represents neither an authentication nor privacy protocol.

Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note
If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication
This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol.You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy
This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

9. In the Storage Type parameter, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

10. Click **Apply** to update the SNMPv3 Target Parameters Table.

11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring the SNMPv3 Community Table

You can create, delete, and modify an SNMPv3 Community Table entry. See the following procedures:

- “Creating an SNMPv3 Community Table Entry” on page 254
- “Deleting an SNMPv3 Community Table Entry” on page 257
- “Modifying an SNMPv3 Community Table Entry” on page 257

For reference information about the SNMPv3 Community Table, see Chapter 21, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Note
Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesis does not recommend this configuration.

Creating an SNMPv3 Community Table Entry

To create an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 97.

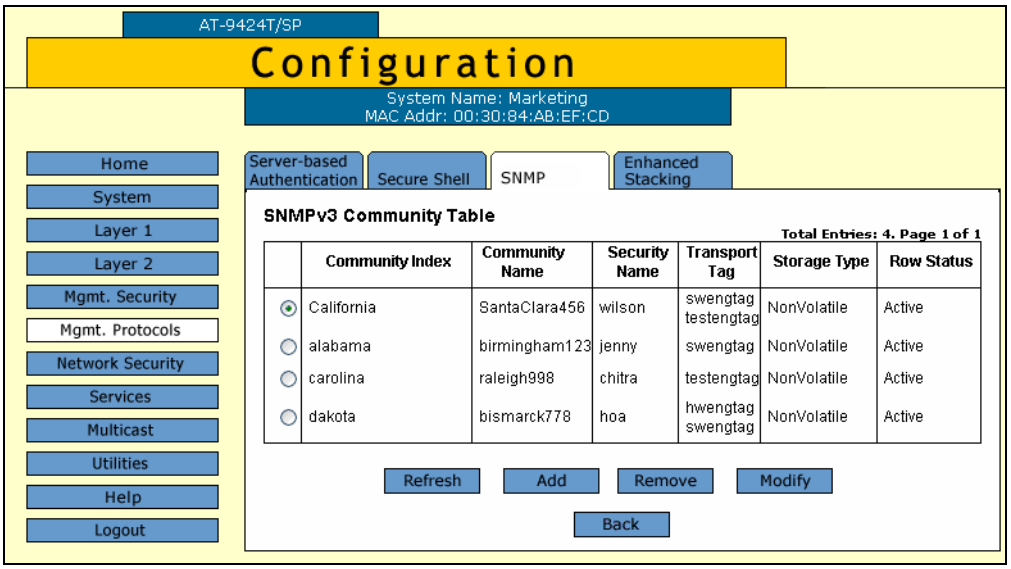

Figure 97. SNMPv3 Community Table Tab (Configuration)

4. Click **Add**.

   The Add New SNMPv3 Community page is shown in Figure 98.

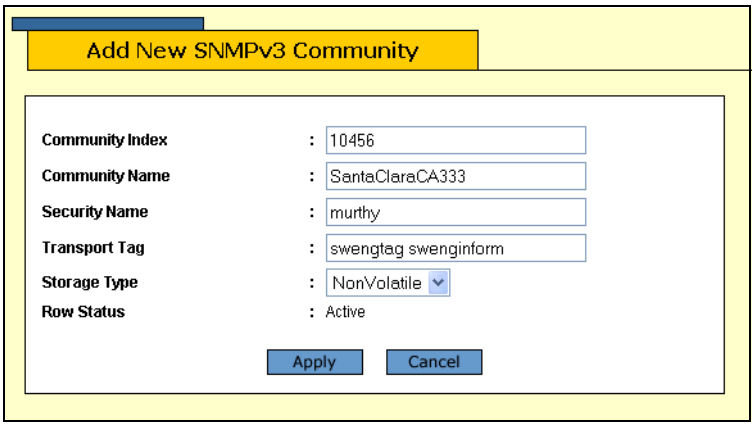

Figure 98. Add New SNMPv3 Community Page

5. In the Community Index field, enter a numerical value for this Community.

   This parameter is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32- alphanumeric characters.

6. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note
Allied Telesis recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

7. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

   This name must be unique. Enter a value of up to 32 alphanumeric characters.

   Note
   Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

8. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See “Creating a Target Address Table Entry” on page 240.

9. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

Note
The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply**.

11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting an SNMPv3 Community Table Entry

To delete an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

   The SNMPv3 Community Table tab is shown in Figure 97 on page 255.

4. Click the button next to the SNMPv3 Community Table entry to be deleted and then click **Remove**.

   A warning message is displayed.

5. Click **OK**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

   The Configuration System page is displayed with the General tab selected by default, as shown in Figure 1 on page 28.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 75 on page 206.

3. In the SNMPv3 section, click the button next to **Configure Community Table**, and then click **Configure** at the bottom of the tab.

   The SNMPv3 Community Table tab is shown in Figure 97 on page 255.

4. Click the button next to the SNMPv3 Community Table entry to be changed and then click **Modify**.

   The Modify SNMPv3 Community page is shown in Figure 99.

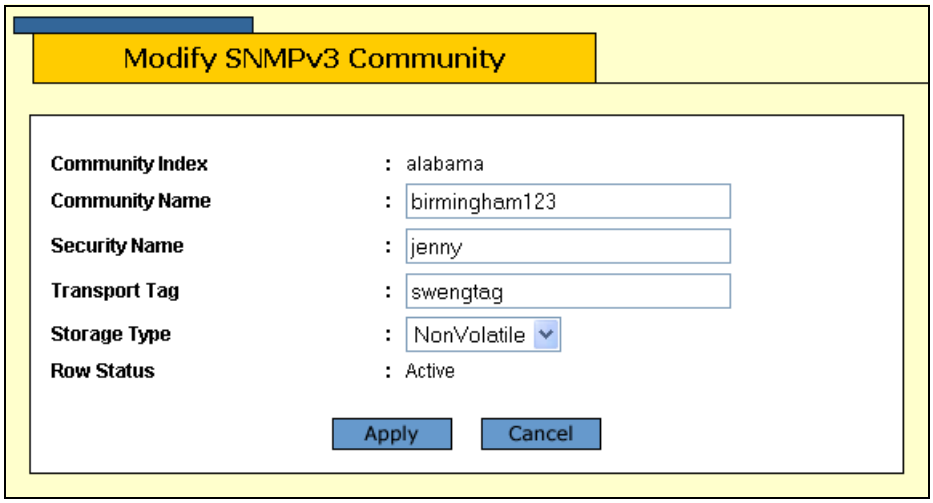

Figure 99. Modify SNMPv3 Community Page

5. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

   The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

   Note
   Allied Telesis recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

6. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

   This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note
Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

7. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

   The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See "Creating a Target Address Table Entry" on page 240.

8. In the Storage Type field, select one of the following storage types for this table entry:

   Volatile
   Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

   NonVolatile
   Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesis recommends this storage type.

   Note
   The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Community Table.

10. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- ❒ “Displaying User Table Entries,” next
- ❒ “Displaying View Table Entries” on page 262
- ❒ “Displaying Access Table Entries” on page 263
- ❒ “Displaying SecurityToGroup Table Entries” on page 264
- ❒ “Displaying Notify Table Entries” on page 265
- ❒ “Displaying Target Address Table Entries” on page 266
- ❒ “Displaying Target Parameters Table Entries” on page 267
- ❒ “Displaying SNMPv3 Community Table Entries” on page 268

Displaying User Table Entries

To display entries in the SNMPv3 User Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Monitoring menu, select **Mgmt. Protocols**.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab displayed by default, as shown in Figure 13 on page 63.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 100.

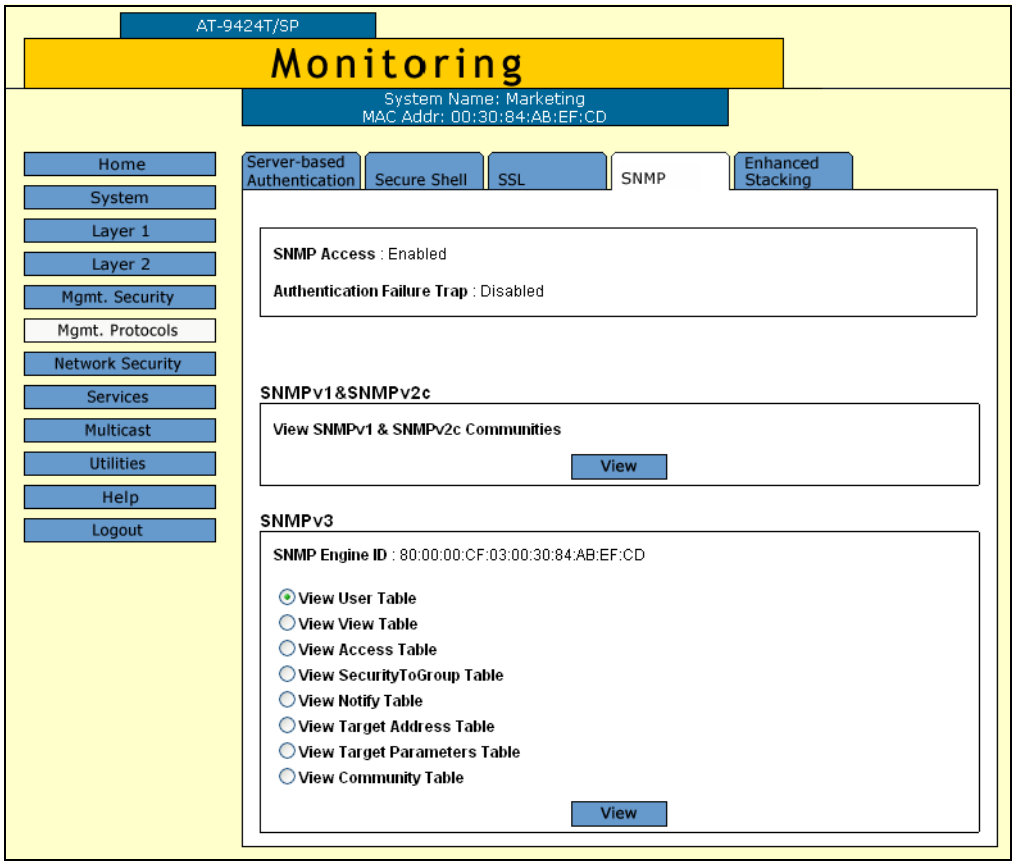

Figure 100. SNMP Tab (Monitoring)

4. In the SNMPv3 section, click the button next to View User Table and then click **View** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 101.

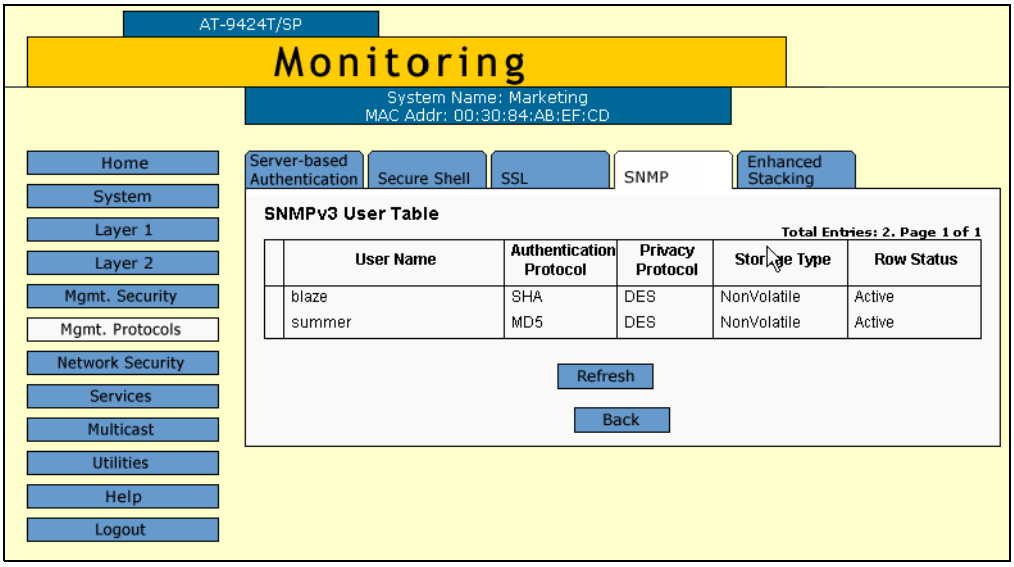

Figure 101. SNMPv3 User Table Tab (Monitoring)

Displaying View Table Entries

To display entries in the SNMPv3 View Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to **View View Table** and then click **View** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 102.

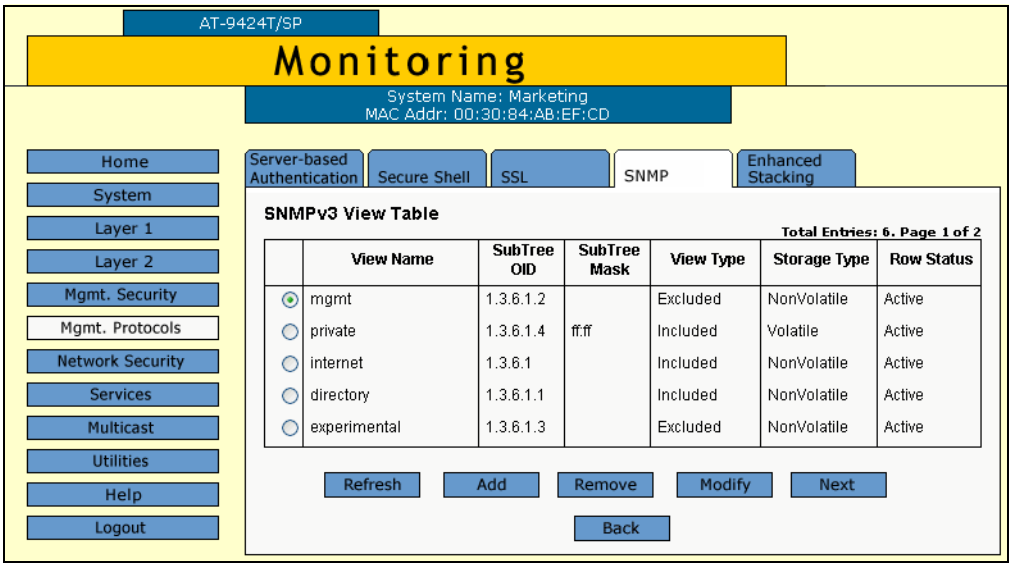

Figure 102. SNMPv3 View Table Tab (Monitoring)

Displaying Access Table Entries

To display entries in the SNMPv3 Access Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to **View Access Table** and then click **View** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 103.

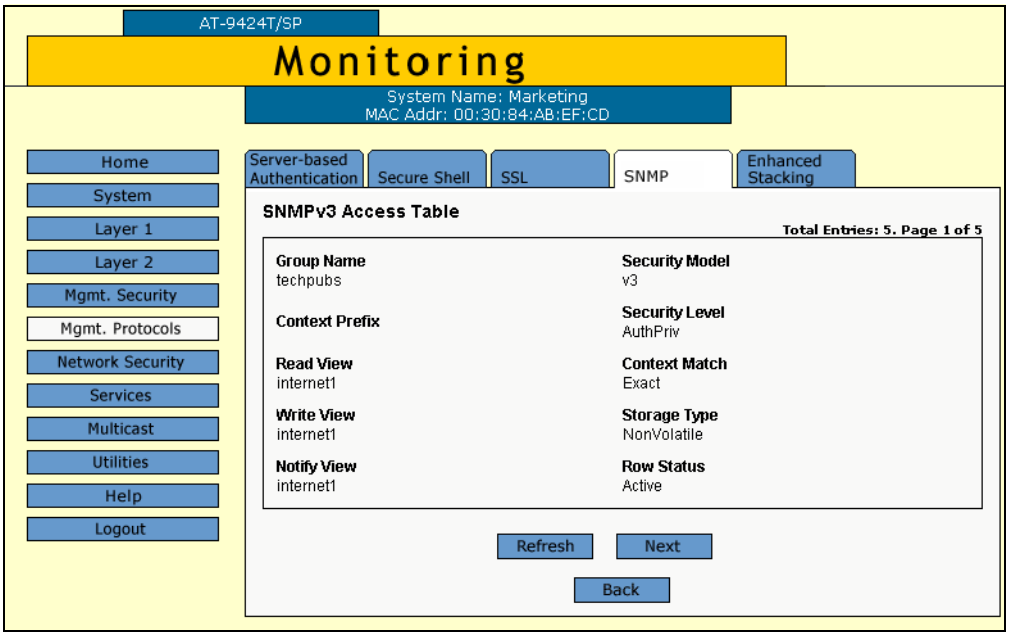

Figure 103. SNMPv3 Access Table Tab (Monitoring)

Displaying SecurityToGroup Table Entries

To display entries in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to the **View SecurityToGroup Table** and then click **View** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 104.

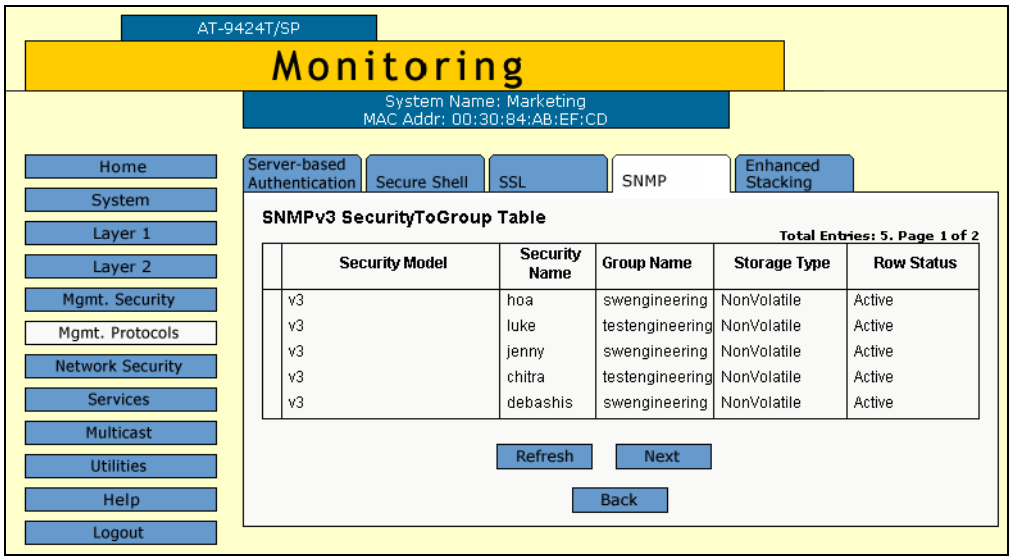

Figure 104. SNMPv3 SecurityToGroup Table Tab (Monitoring)

Displaying Notify Table Entries

To display entries in the SNMPv3 Notify Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to **View Notify Table** and then click **View** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 105.

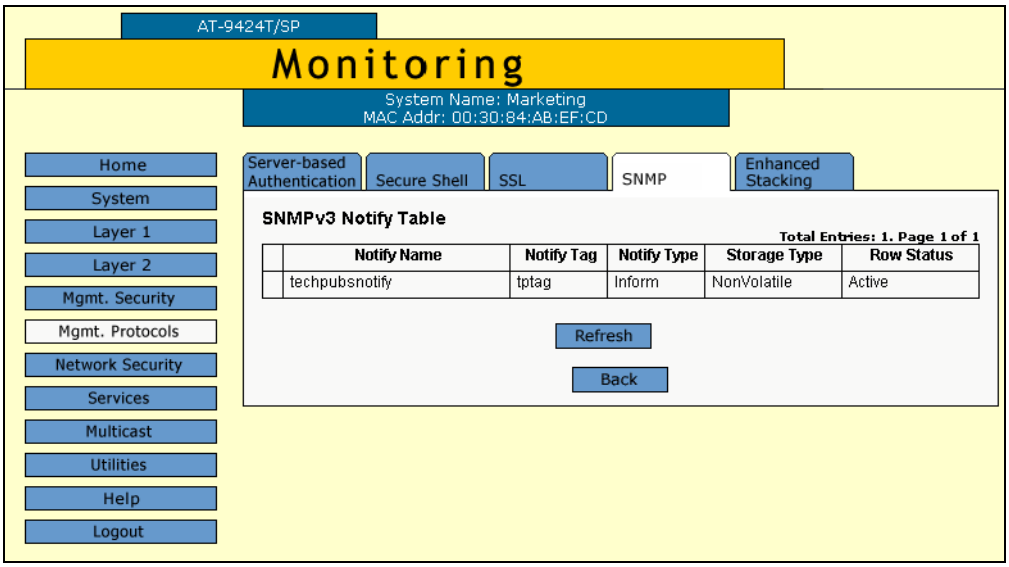

Figure 105. SNMPv3 Notify Table Tab (Monitoring)

Displaying Target Address Table Entries

To display entries in the SNMPv3 Target Address Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** Tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, lick the button next to **View Target Address Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 106.

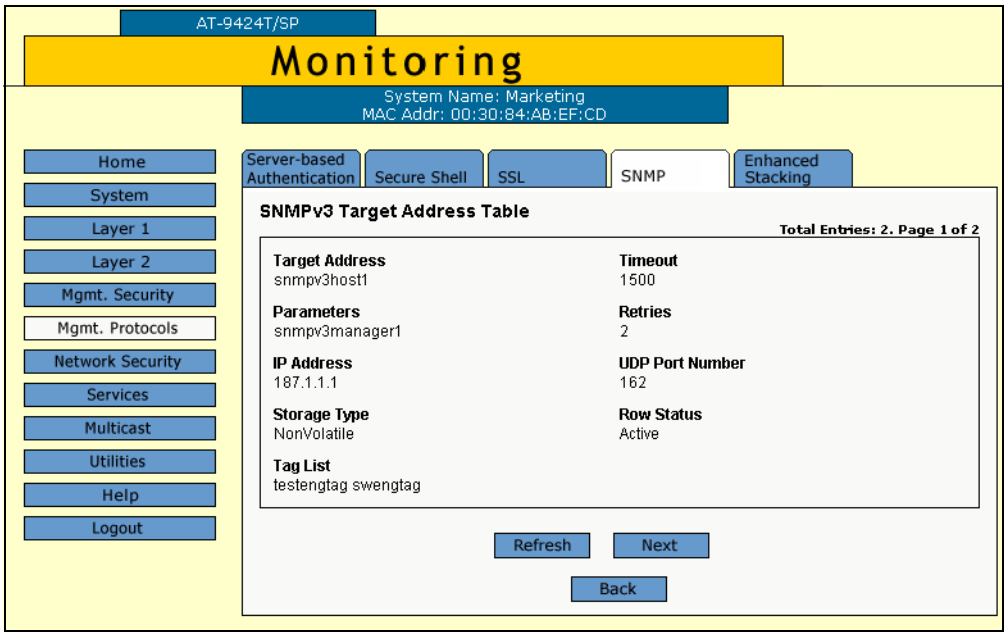

Figure 106. SNMPv3 Target Address Table Tab (Monitoring)

Displaying Target Parameters Table Entries

To display entries in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to the **View Target Parameters Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 107.

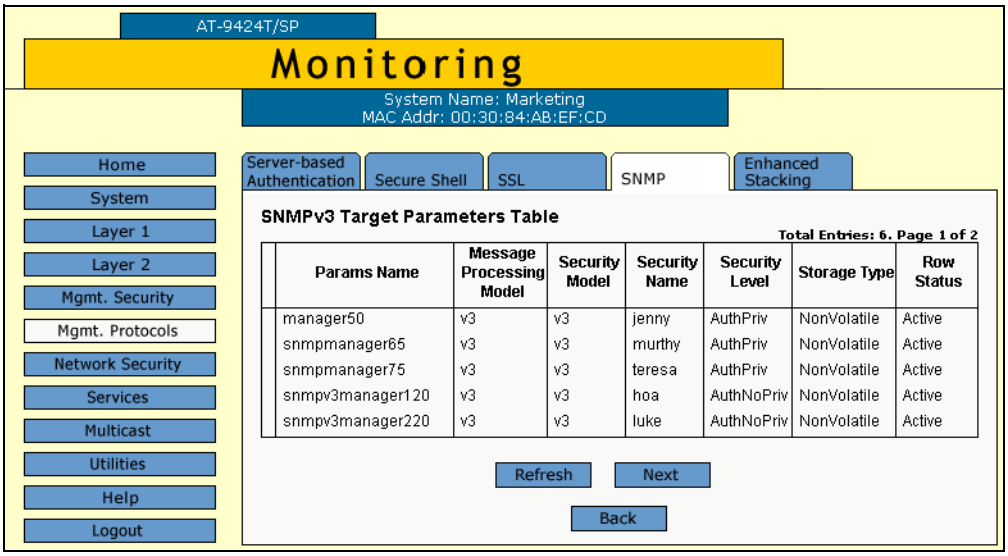
AT-9424T/SP
Monitoring
System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD
Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout
Server-based Authentication
Secure Shell
SSL
SNMP
Enhanced Stacking
SNMPv3 Target Parameters Table
Total Entries: 6. Page 1 of 2
Params Name | Message Processing Model | Security Model | Security Name | Security Level | Storage Type | Row Status
manager50 | v3 | v3 | jenny | AuthPriv | NonVolatile | Active
snmpmanager65 | v3 | v3 | murthy | AuthPriv | NonVolatile | Active
snmpmanager75 | v3 | v3 | teresa | AuthPriv | NonVolatile | Active
snmpv3manager120 | v3 | v3 | hoa | AuthNoPriv | NonVolatile | Active
snmpv3manager220 | v3 | v3 | luke | AuthNoPriv | NonVolatile | Active
Refresh
Next
Back

Figure 107. SNMPv3 Target Parameters Table Tab (Monitoring)

Displaying SNMPv3 Community Table Entries

To display entries in the SNMPv3 Community Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

   The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

   The SNMP tab is shown in Figure 100 on page 261.

3. In the SNMPv3 section, click the button next to **View Community Table** and then click **View** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 108.

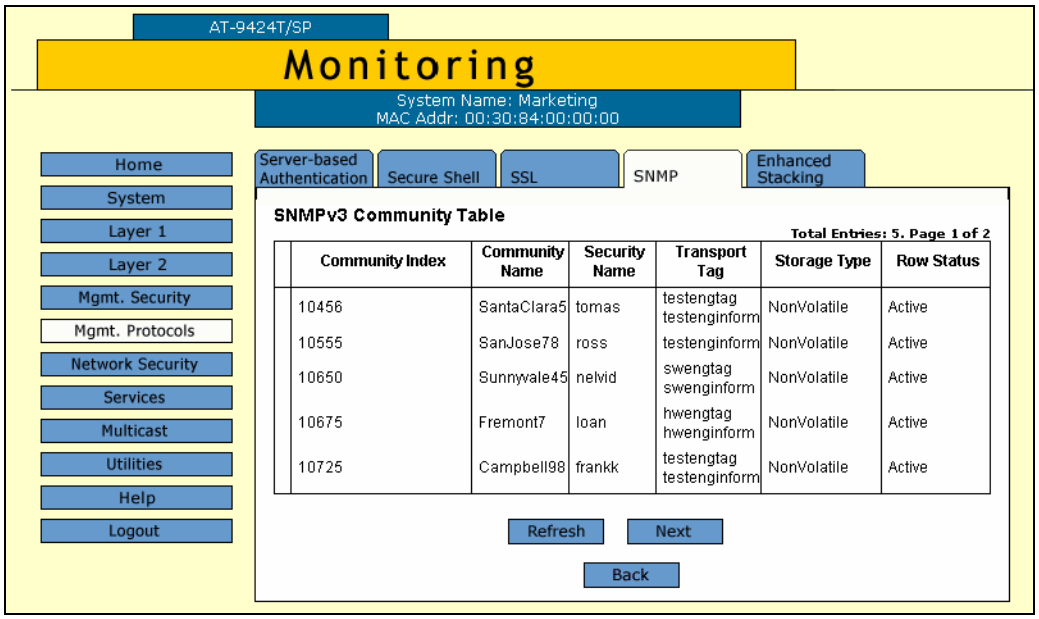

Figure 108. SNMPv3 Community Table Tab (Monitoring)

Section IV

Spanning Tree Protocols

This section has the following chapters:

- Chapter 18, “Spanning Tree and Rapid Spanning Tree Protocols” on page 273
- Chapter 19, “Multiple Spanning Tree Protocol” on page 293

Chapter 18

Spanning Tree and Rapid Spanning Tree Protocols

This chapter explains how to configure the STP and RSTP parameters on an AT-9400 Series switch. The sections in the chapter include:

- “Enabling or Disabling a Spanning Tree Protocol” on page 274
- “Configuring STP” on page 276
- “Configuring RSTP” on page 284

Enabling or Disabling a Spanning Tree Protocol

To enable or disable spanning tree on the switch or to select the active spanning tree protocol, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109.

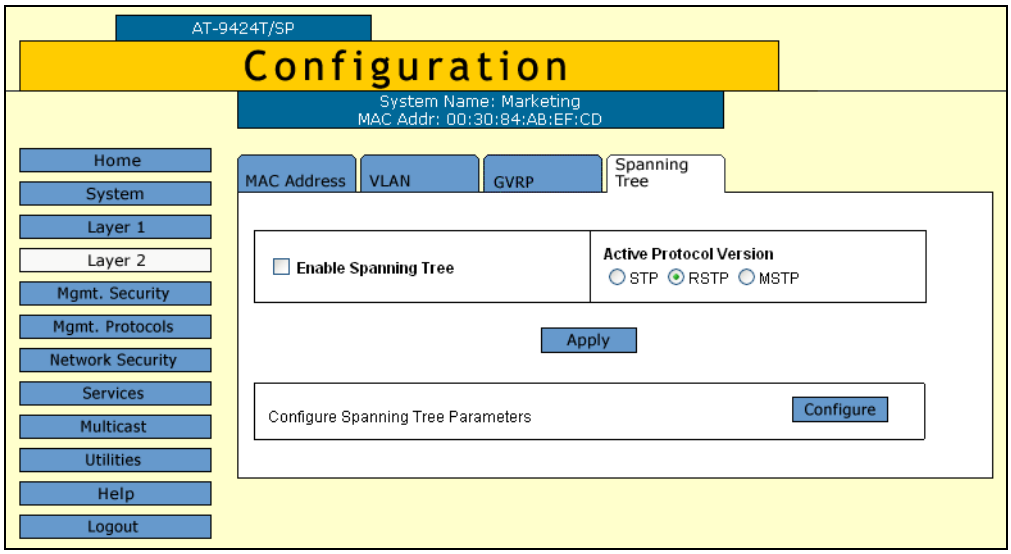

Figure 109. Spanning Tree Tab (Configuration)

4. To select a spanning tree version, from the Active Protocol Version parameter click **STP**, **RSTP**, or **MSTP**. The default is RSTP.

   Note
   Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.
6. Click **Apply**.

   A change to the status of the spanning tree protocol is immediately implemented on the switch.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

8. If you activated STP, go to "Configuring STP" on page 276. If you activated RSTP go to Step "Configuring RSTP" on page 284. If you activated MSTP, go to Chapter 19, "Multiple Spanning Tree Protocol" on page 293.

Configuring STP

This section contains the following procedures:

- ”Configuring STP Bridge Settings”, next
- “Configuring STP Port Settings” on page 279
- “Displaying the STP Settings” on page 280
- “Resetting STP to the Default Settings” on page 282

Caution
The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

Configuring STP Bridge Settings

To configure STP bridge settings, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.
4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 110.

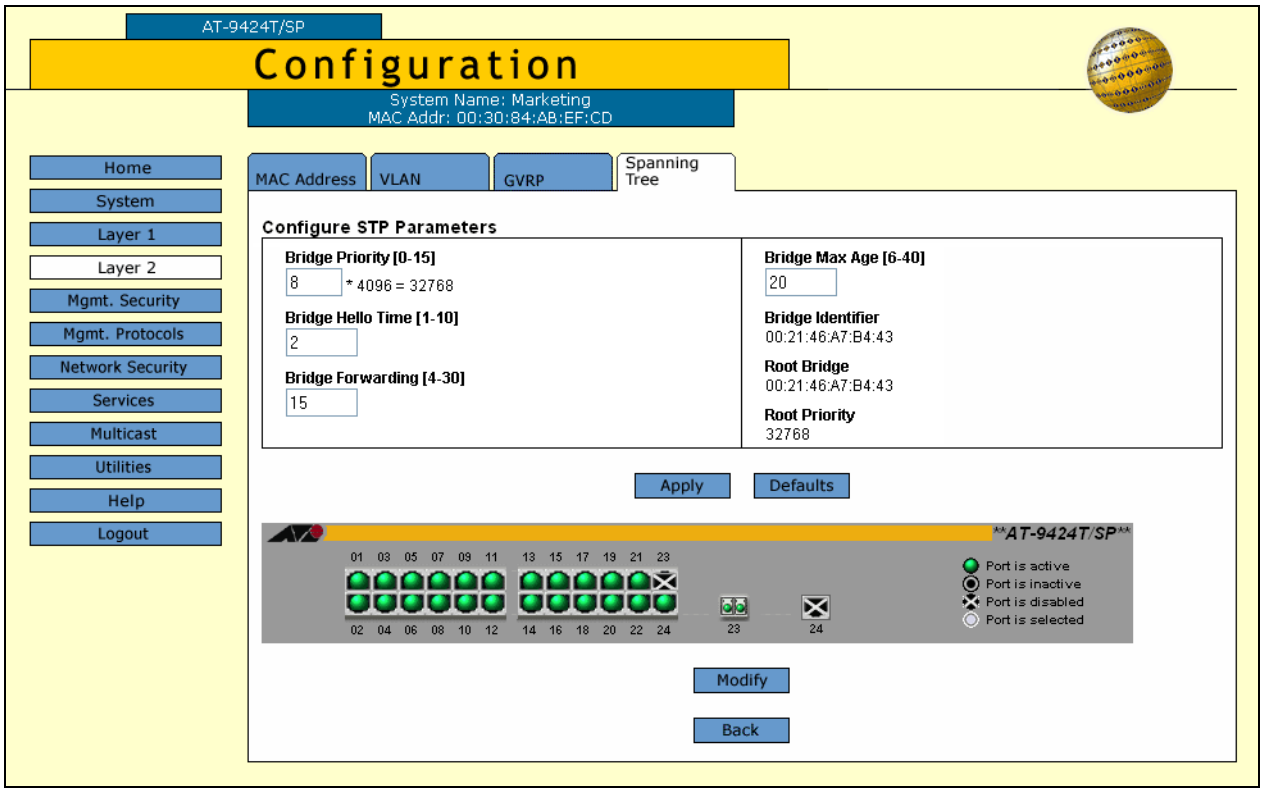

Figure 110. Configure STP Parameters Tab (Configuration)

Note
The Defaults button returns all STP settings to the default settings.

5. Configure the following parameters as necessary.

   Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 5.

Table 5. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding Delay
The waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

In selecting a value for maximum age, the following rules must be observed:

MaxAge must be greater than (2 x (HelloTime + 1))

MaxAge must be less than (2 x (ForwardingDelay - 1))

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

Root Bridge
The MAC address of the root bridge of the spanning tree domain. This value cannot be changed and is only displayed when STP is activated on the switch.

Root Priority
The priority value on the root bridge of the spanning tree domain. This parameter is only displayed when STP is enabled on the switch. To change the priority value on the root bridge, you must start a management session on the switch functioning as the root bridge and change its bridge priority value.

6. After you have made the desired changes, click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring STP Port Settings

To configure STP port parameters, perform the following procedure:

1. Perform steps 1 to 4 in "Configuring STP Bridge Settings" on page 276 to display the Spanning Tree tab.

2. To configure a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The STP Settings - Port(s) page is shown in Figure 111.

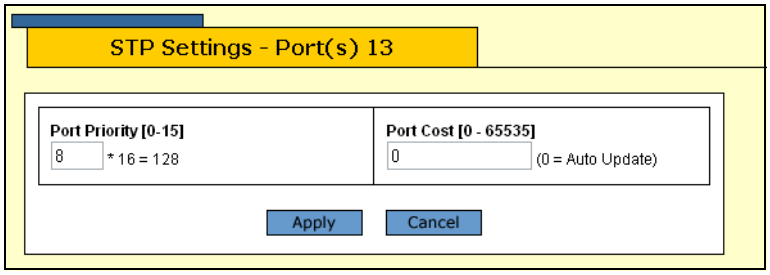

Figure 111. STP Settings - Port(s) Page

3. Configure the following parameters as necessary.

Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 6 on page 280.

Table 6. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 65,535. The default setting is Auto-detect, which sets port cost depending on the speed of the port. If you select Auto-Detect, the management software assigns a value of 100 if the port is operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

4. After you have configured the parameters, click **Apply**.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the STP Settings

To display the STP settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

The Spanning Tree tabs is shown in Figure 112.

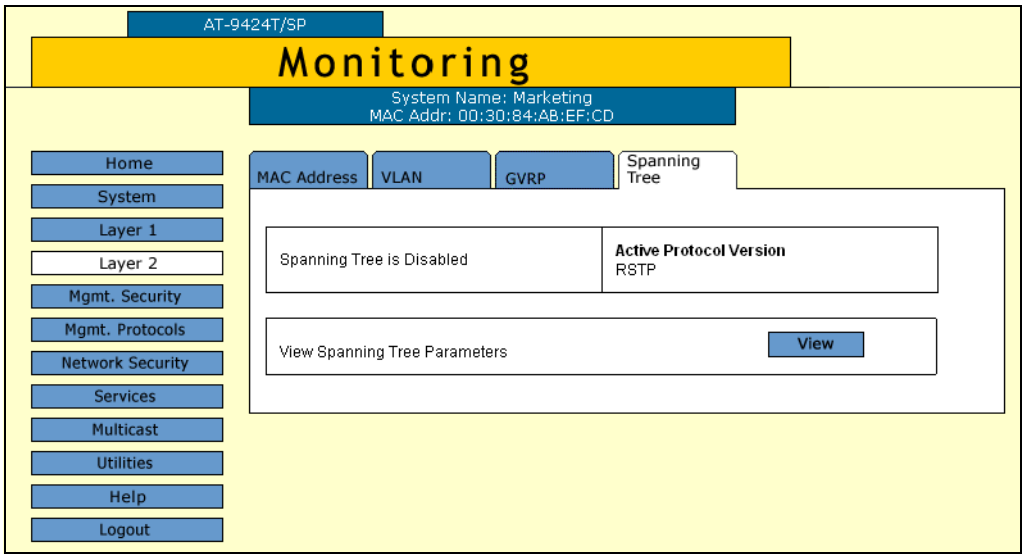

Figure 112. Spanning Tree Tab (Monitoring)

4. Click **View**.

The Monitor STP Parameters tab is shown in Figure 113.

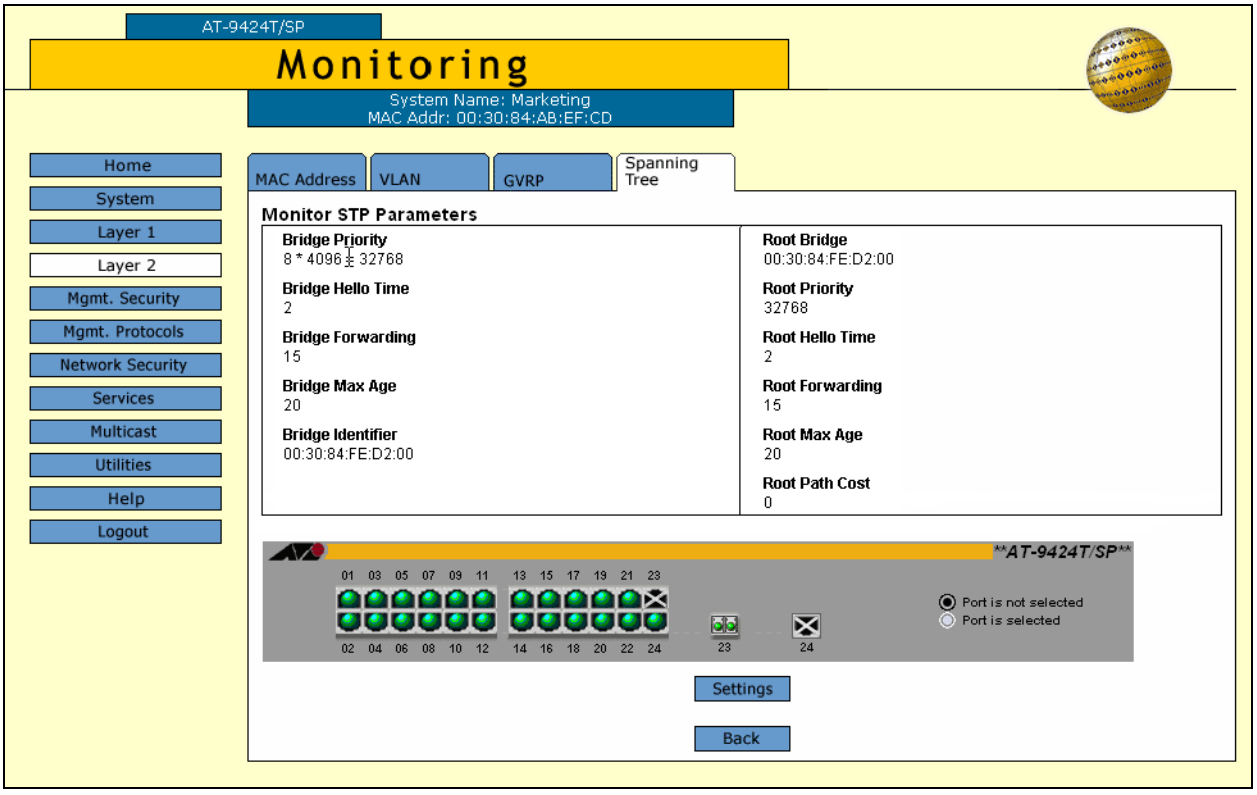

Figure 113. Monitor STP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

   The STP Settings page is shown in Figure 114.

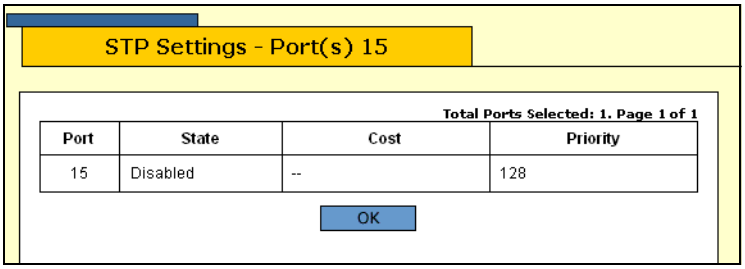

Figure 114. STP Settings Page

   The STP Settings page displays a table that contains the following columns of information:

   Port
   The port number.

   State
   Current state of a port. The possible states are Listening, Learning, Forwarding, or Blocking when spanning tree is enabled on the switch. When spanning tree is not enabled on the switch or if a port is not being used, its state will be disabled.

   Cost
   Port cost of the port.

   Priority
   The port's priority value. The number is used as a tie breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Resetting STP to the Default Settings

To reset STP to the factory default settings, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.

4. Verify there is no check in the **Enable Spanning Tree** check box. If there is a check, click the option to remove it. Spanning tree must be disabled in order for you to return it to its default settings.

5. Click **Configure**.

   The Configure STP Parameters tab is shown in Figure 110 on page 277.

6. Click **Defaults**.

   The STP settings are returned to their default values.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring RSTP

This section contains the following procedures:

- ”Configuring RSTP Bridge Settings”, next
- “Configuring RSTP Port Settings” on page 287
- “Displaying RSTP Settings” on page 288
- “Resetting RSTP to the Default Settings” on page 291

Caution
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

Configuring RSTP Bridge Settings

To configure RSTP bridge parameters, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.
4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 115.

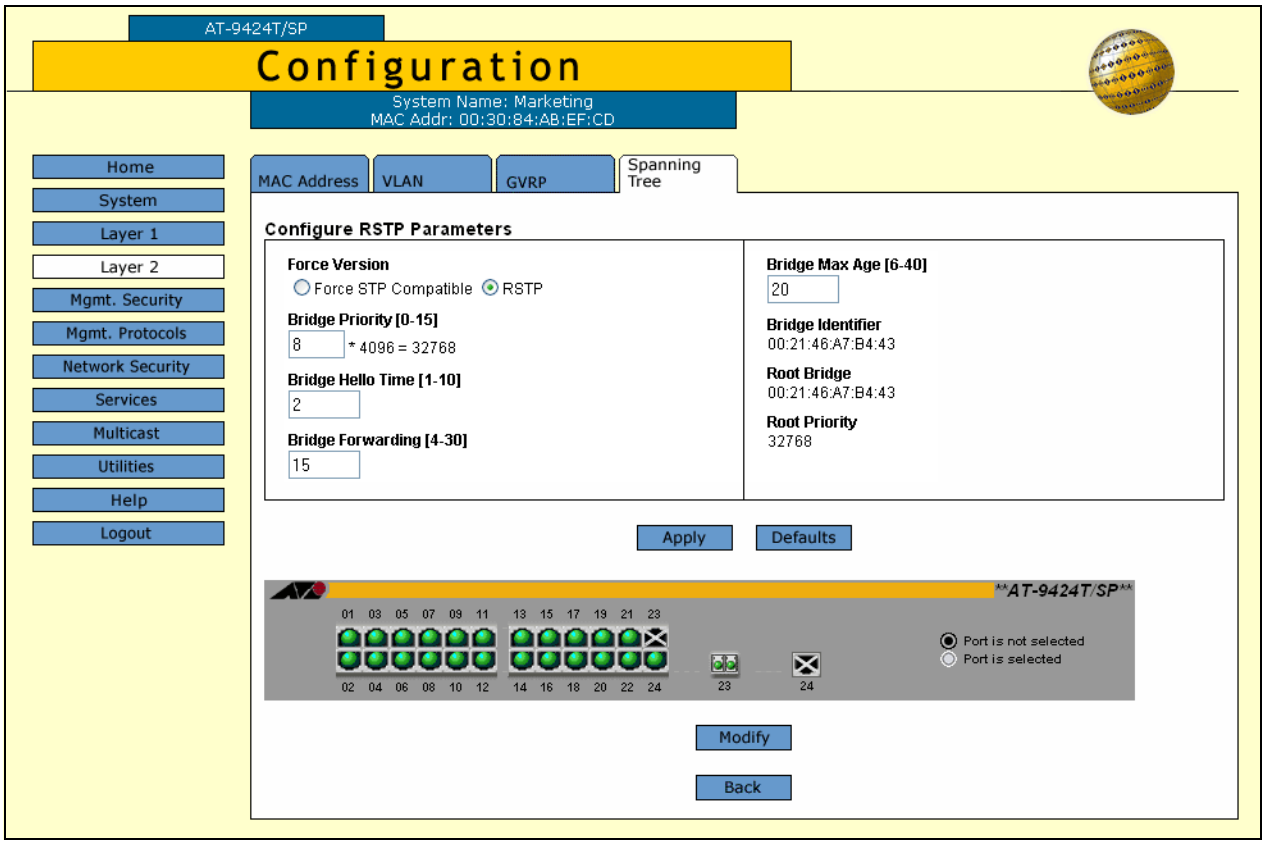

Figure 115. Configure RSTP Parameters Tab (Configuration)

5. Configure the following parameters as necessary.

Force Version
This selection determines whether the bridge operates with RSTP or in an STP-compatible mode. If you select RSTP, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge operates in RSTP, using the RSTP parameter settings, but it sends only STP BPDU packets out the ports.

Bridge Priority
The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 5 on page 278.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding
The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1)).

MaxAge must be less than (2 x (ForwardingDelay - 1))

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

Root Bridge
The MAC address of the root bridge of the spanning tree domain. This value cannot be changed and is only displayed when RSTP is activated on the switch.

Root Priority
The priority value on the root bridge of the spanning tree domain. This parameter is only displayed when RSTP is enabled on the switch. To change the priority value on the root bridge, you must start a management session on the switch functioning as the root bridge and change its bridge priority value.

6. After you have made your changes, click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring RSTP Port Settings

To configure RSTP port parameters, perform the following procedure:

1. Perform steps 1 to 4 in "Configuring RSTP Bridge Settings" on page 284 to display the Spanning Tree tab.

2. To configure RSTP port settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The RSTP Settings - Port(s) page is shown in Figure 116.

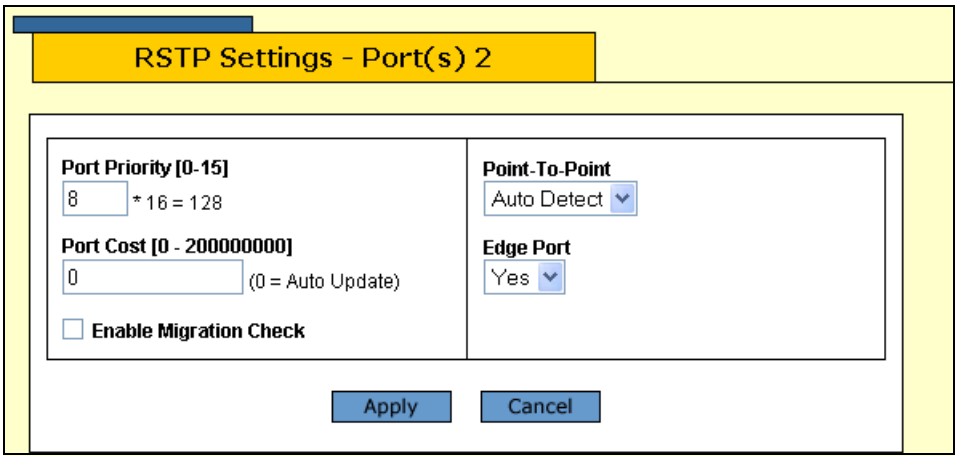

Figure 116. RSTP Settings - Port(s) Page

3. Configure the following parameters as necessary.

   Port Priority
   This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to Table 6 on page 280.

   Port Cost
   The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

   Enable Migration Check
   This parameter is displayed only when RSTP is enabled. This parameter resets an RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely. Type C to reset the MSTP port to transmit RSTP BPDUs.

Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 22, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Features Guide*.

Edge Port
This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 22, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Features Guide*.

4. After you have configured the parameters, click **Apply**.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying RSTP Settings

To display RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tabs is shown in Figure 112 on page 281.

   This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.
4. Click **View**.

The Monitor RSTP Parameters tab is shown in Figure 117.

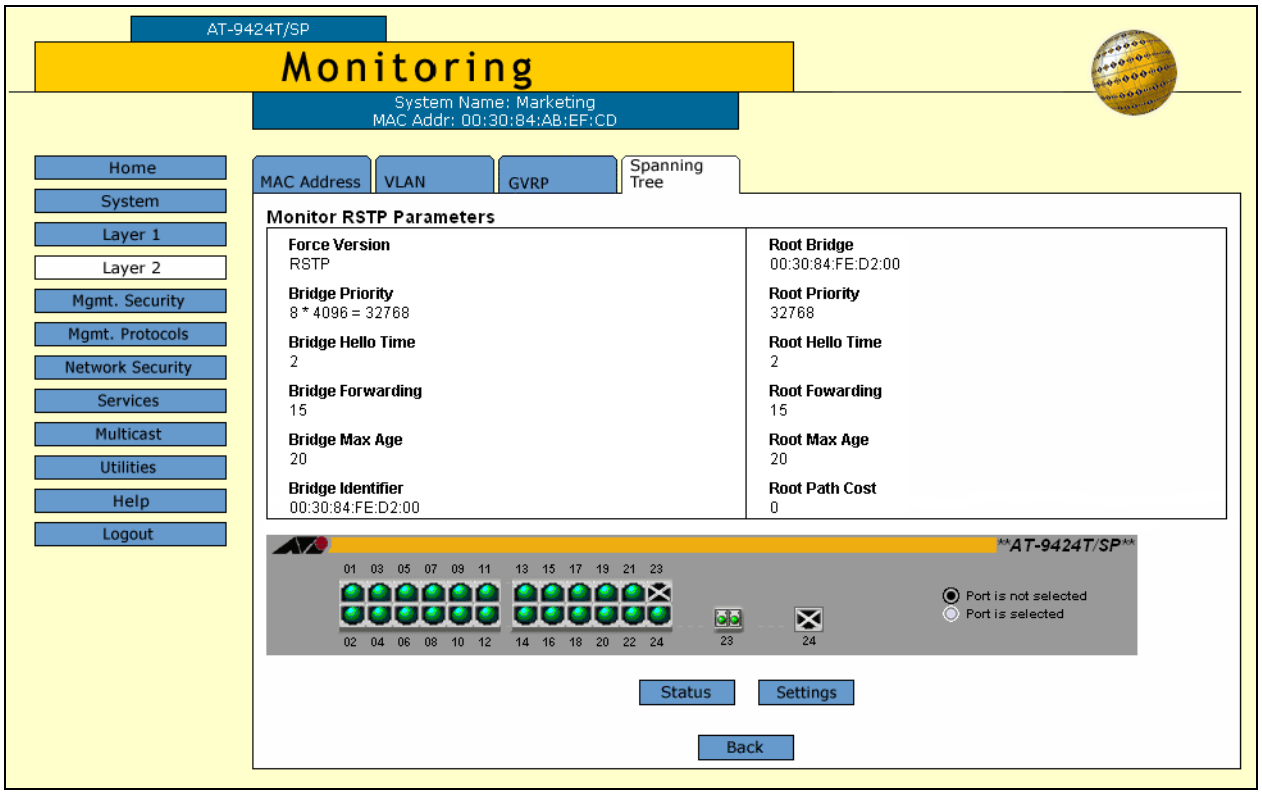

Figure 117. Monitor RSTP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch image and click **Status** or **Settings**. You can select more than one port.

   An example of the RSTP Status page is shown in Figure 119.

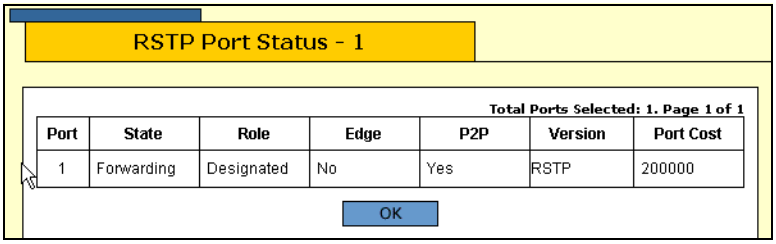

Figure 118. RSTP Port Status Page

The RSTP Port Status page displays a table that contains the following columns of information:

Port
The port number.

State
The RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding.

The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Blocking.

The possible states for a port not being used or where spanning tree is not activated is Disabled.

Role
The RSTP role of the port. Possible roles are:

Root - The port that is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path in the direction of the root switch.

Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Edge-Port
Whether or not the port is operating as an edge port. The possible settings are Yes and No.

P2P
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes and No.

Version
Whether the port is operating in RSTP mode or STP-compatible mode.

Port Cost
The port cost of the port.

An example of the RSTP Settings page is shown in Figure 119.

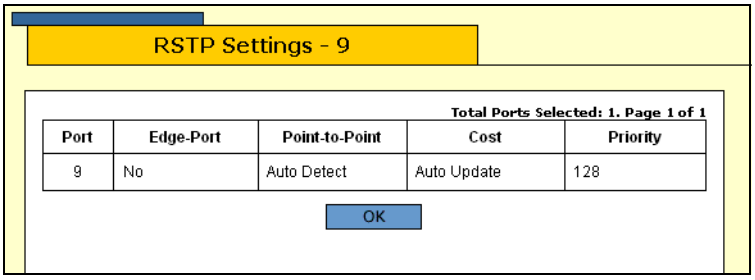

Figure 119. RSTP Settings Page

The RSTP Settings page displays a table with the following columns of information:

Port
The port number.

Edge-Port
Whether or not the port is operating as an edge port. The possible settings are Yes and No.

Point-to-Point
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto Detect.

Cost
Port cost of the port. The default is Auto Update.

Priority
The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Resetting RSTP to the Default Settings

To reset RSTP to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.

4. Verify that there is no check in the **Enable Spanning Tree** check box. If there is a check, click the option to remove it. Spanning tree must be disabled in order for you to return it to its default settings.
5. Click **Configure**.

   The Configure RSTP Bridge Parameters tab is shown in Figure 115 on page 285.

6. Click **Defaults**.

   The RSTP settings are returned to their default values.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Chapter 19

Multiple Spanning Tree Protocol

This chapter explains how to configure multiple spanning tree protocol (MSTP) parameters on the AT-9400 Switch using a web browser management session. It contains the following procedures:

- ❒ “Enabling MSTP” on page 294
- ❒ “Configuring MSTP” on page 296
- ❒ “Managing MSTIs” on page 300
- ❒ “Configuring MSTP Port Parameters” on page 304
- ❒ “Displaying the MSTP Configuration” on page 308
- ❒ “Resetting MSTP to the Default Settings” on page 313

Enabling MSTP

The AT-9400 Switch can support the three spanning tree protocols STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. After you select it, you can then enable or disable it.

To select MSTP as the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note
Changing the active spanning tree protocol resets the switch.

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 120.

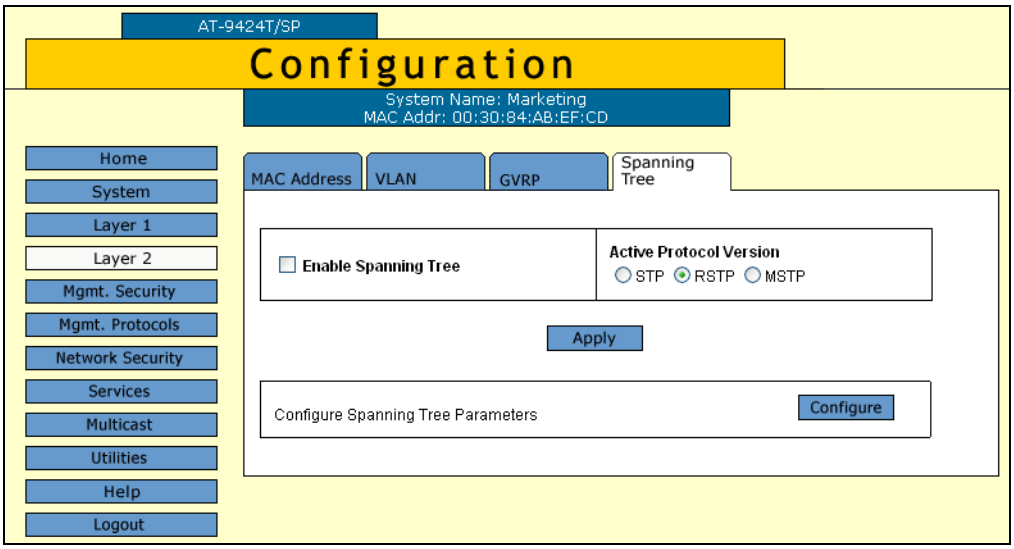

Figure 120. Spanning Tree Tab (Configuration)

Note
If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to Step 5.

4. To change the active spanning tree protocol on the switch, click **STP**, **RSTP**, or **MSTP** in the Active Protocol Version section of the tab. The default is RSTP.

   Note
   Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable the active spanning tree protocol on the switch, click the **Enable Spanning Tree** check box. A check indicates that the spanning tree is enabled while no check indicates that spanning tree is disabled. The default is disabled.

6. Click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

8. If you activated STP, go to "Configuring STP" on page 276. If you activated RSTP go to "Configuring RSTP" on page 284. If you activated MSTP, go to "Configuring MSTP" on page 296.

Configuring MSTP

This section contains the following procedures:

- ❒ “Configuring MSTP Parameters,” next
- ❒ “Configuring the CIST Priority” on page 299
- ❒ “Managing MSTIs” on page 300
- ❒ “Configuring MSTP Port Parameters” on page 304

Note
MSTP must be selected as the active spanning tree protocol on the switch before you can configure it. For instructions on selecting the active spanning tree, refer to “Enabling MSTP” on page 294.

Note
When MSTP is enabled, the GVRP tab is not shown on the Configuration or Monitoring Layer 2 page.

Configuring MSTP Parameters

To configure MSTP parameters, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.
4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121.

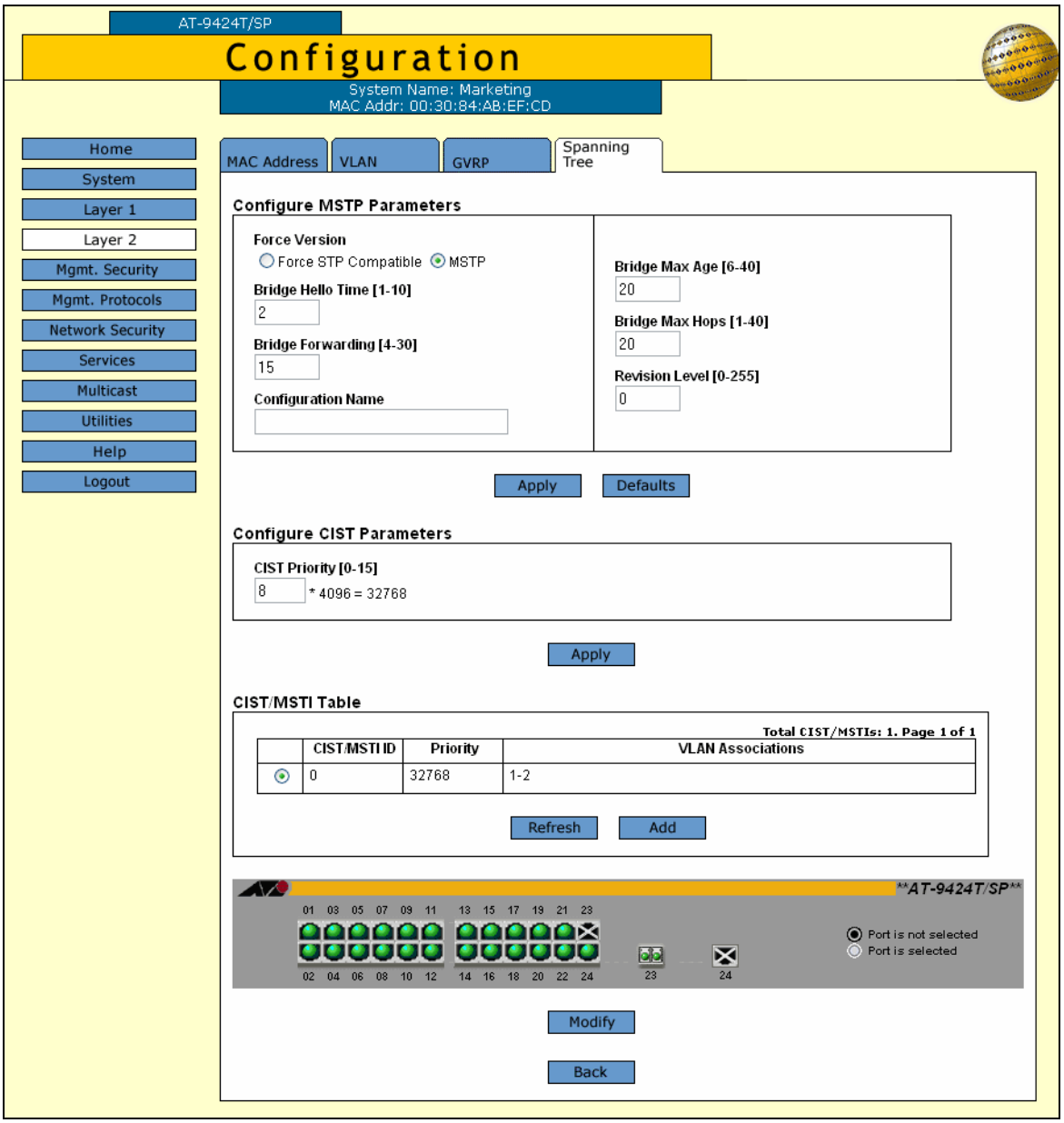

Figure 121. Configure MSTP Parameters Tab (Configuration)

Note

This procedure explains the Configure MSTP Parameters section of the page. The CIST/MSTI Table is explained in "Creating an MSTI" on page 300, "Modifying an MSTI" on page 301, and "Deleting an MSTI" on page 302. The graphic image of the switch is described in "Configuring MSTP Port Parameters" on page 304.

Configure the following parameters as necessary.

Force Version
This selection determines whether the bridge operates with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

Note
Selecting the STP-compatible mode deletes all spanning tree instances on the switch.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

Bridge Forwarding
The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Configuration Name
The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

Bridge Max Age
The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than (2 x (HelloTime + 1))

MaxAge must be less than (2 x (ForwardingDelay - 1))

Bridge Max Hops
MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. After the counter reaches zero, the BPDU is deleted.

Revision Level
The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

5. Click **Apply**.
6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

   Proceed to the next procedure to configure the CIST priority.

Configuring the CIST Priority

To configure the CIST priority, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.

5. In the Configure CIST Parameters section, set the **CIST Priority**, the priority number for the bridge.

   This number is used to determine the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Click **Apply**.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Managing MSTIs

This section contains the following procedures:

- ❒ “Creating an MSTI” on page 300
- ❒ “Modifying an MSTI” on page 301
- ❒ “Deleting an MSTI” on page 302

Creating an MSTI

To create an MSTI, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.
4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.
5. In the CIST/MSTI Table section of the tab, click **Add**.

   The Add New MSTI page is shown in Figure 122.

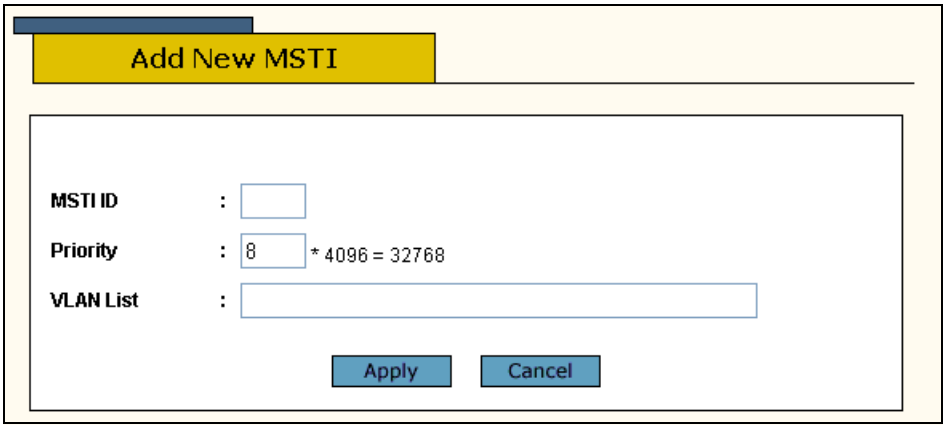

Figure 122. Add New MSTI Page

6. In the MSTI ID field, enter an ID number for the MSTI. The range is 1 to 15.

7. In the Priority field, enter an MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to Table 5, "Bridge Priority Value Increments" on page 278. The default is 0.

8. To add VLANs to the MSTI, enter the VIDs in the VLAN List field. Separate multiple VIDs with a comma.

9. Click **Apply**.

   The management software creates the MSTI.

10. Repeat steps 5 to 9 to create additional MSTIs.

11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying an MSTI

To modify an MSTI, perform the following procedure:

1. From the home page, select **Configuration**.

2. From the Configuration menu, select the **Layer 2** option.

3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.

4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.

5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID to be modified. You can only modify one MSTI ID at a time. You cannot modify CIST.

6. Click **Modify**.

The Modify MSTI page is shown in Figure 123.

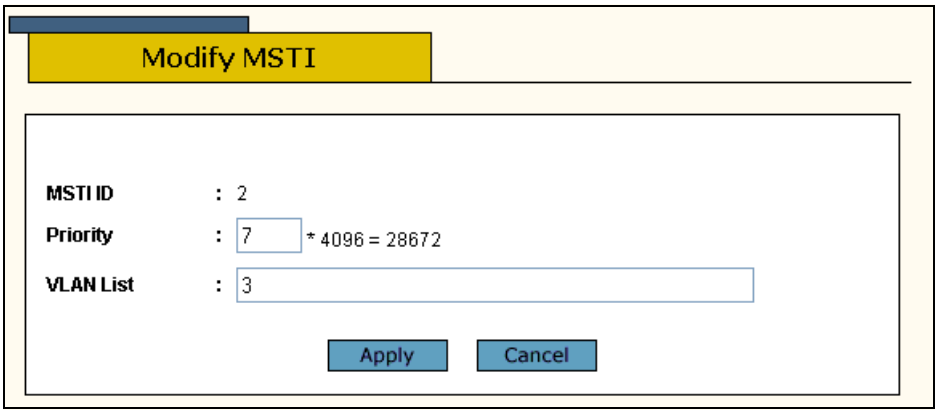

Figure 123. Modify MSTI Page

7. To change the MSTI's priority value, enter a value in the Priority field. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer toTable 5, "Bridge Priority Value Increments" on page 278. The default is 0.
8. To add or remove VLANs from the MSTI, edit the VIDs in the VLAN List field. Separate multiple VIDs with a comma.
9. Click **Apply**.
10. Repeat steps 5 to 9 to modify additional MSTIs.
11. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting an MSTI

To delete an MSTI, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.
4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.
5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI to be deleted. You can only delete one MSTI at a time.
6. Click **Remove**.

7. A confirmation prompt is displayed.
8. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure.

   If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.
9. Repeat steps 5 to 8 to delete additional MSTIs.
10. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 120 on page 294.
4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.
5. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded page, click the port to be configured. You can configure more than one port at a time.
6. Click **Modify**.

   The MSTP Settings - Port(s) page is shown in Figure 124.

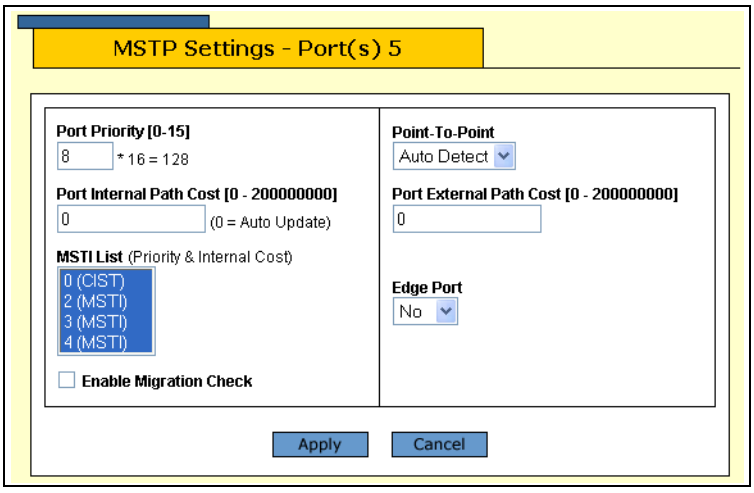

Figure 124. MSTP Settings - Port(s) Page

7. Configure the following parameters as necessary.

   The port parameters can be divided into two groups: generic parameters and MSTI-specific parameters. A generic port parameter is set just once on a port and applies to all of a port's MSTIs assignments. Generic parameters are:

   - External path cost

- Point-to-point port
- Edge port

An MSTI-specific parameter can be set on a per MSTI basis. This means that you can assign a different value to a MSTI-specific parameter for each spanning tree instance where a port is a member. These parameters are:

- Internal path cost
- Port priority

When setting an MSTI-specific parameter, use the MSTI List in the window to select the intended MSTI. It should be noted that the MSTI List shows all of the spanning tree instances on the switch, and not just those where the selected port is currently a member. If you select an MSTI where the port is not a member, you can pre-configure the parameter in the event you later add the port as a member of the MSTI through a VLAN assignment.

Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value is 128). For a list of the increments, refer to Table 6, "Port Priority Value Increments" on page 280.

Port Internal Path Cost
The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Table 7 lists the MSTP port cost with Auto Update when a port is not part of a port trunk.

Table 7. MSTP Auto Update Port Internal Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 8 lists the MSTP port costs with Auto Update when the port is part of a port trunk.

Table 8. MSTP Auto Update Port Trunk Internal Path Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000

Table 8. MSTP Auto Update Port Trunk Internal Path Costs

Port Speed	Port Cost
1000 Mbps	2,000

MSTI List
The MSTIs defined on the switch. You can use this list when setting the port priority and port internal path cost parameters to assign different values to a port for each MSTI when the port is a member. Before setting priority or internal path cost, select the appropriate MSTI where you want the new setting to be applied on the port. The default is all MSTIs on the switch.

The MSTI List shows all of the spanning tree instances on the switch, and not just those where the selected port is currently a member. If you select an MSTI where the port is not a member, you can pre-configure the parameter in the event you later add the port as a member of the MSTI through a VLAN assignment.

Enable Migration Check
This parameter is displayed only when MSTP is enabled. This parameter resets a port, allowing it to send RSTP BPDUs. When an MSTP bridge receives STP BPDUs on an MSTP port, the port transmits STP BPDUs. The port continues to transmit STP BPDUs indefinitely.

Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 22, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Features Guide*.

Port External Path Cost
The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. Table 9 on page 306 lists the MSTP port costs with the Auto setting when the port is not a member of a trunk.

Table 9. MSTP Auto External Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 10 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 10. MSTP Auto External Path Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

Edge Port
This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to "Point-to-Point and Edge Ports" in Chapter 22, "Spanning Tree and Rapid Spanning Tree Protocols" in the *AT-S63 Management Software Features Guide*.

8. After configuring the parameters, click **Apply**.
9. To permanently save your changes, select the **Save Config** option in the Configuration menu.
10. Repeat this procedure to configure the MSTP parameters for other switch ports.

Displaying the MSTP Configuration

To display the MSTP configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 109 on page 274.

   This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP, RSTP, or MSTP is active.
4. Click **View**.

The MSTP Parameters tab is shown in Figure 125.

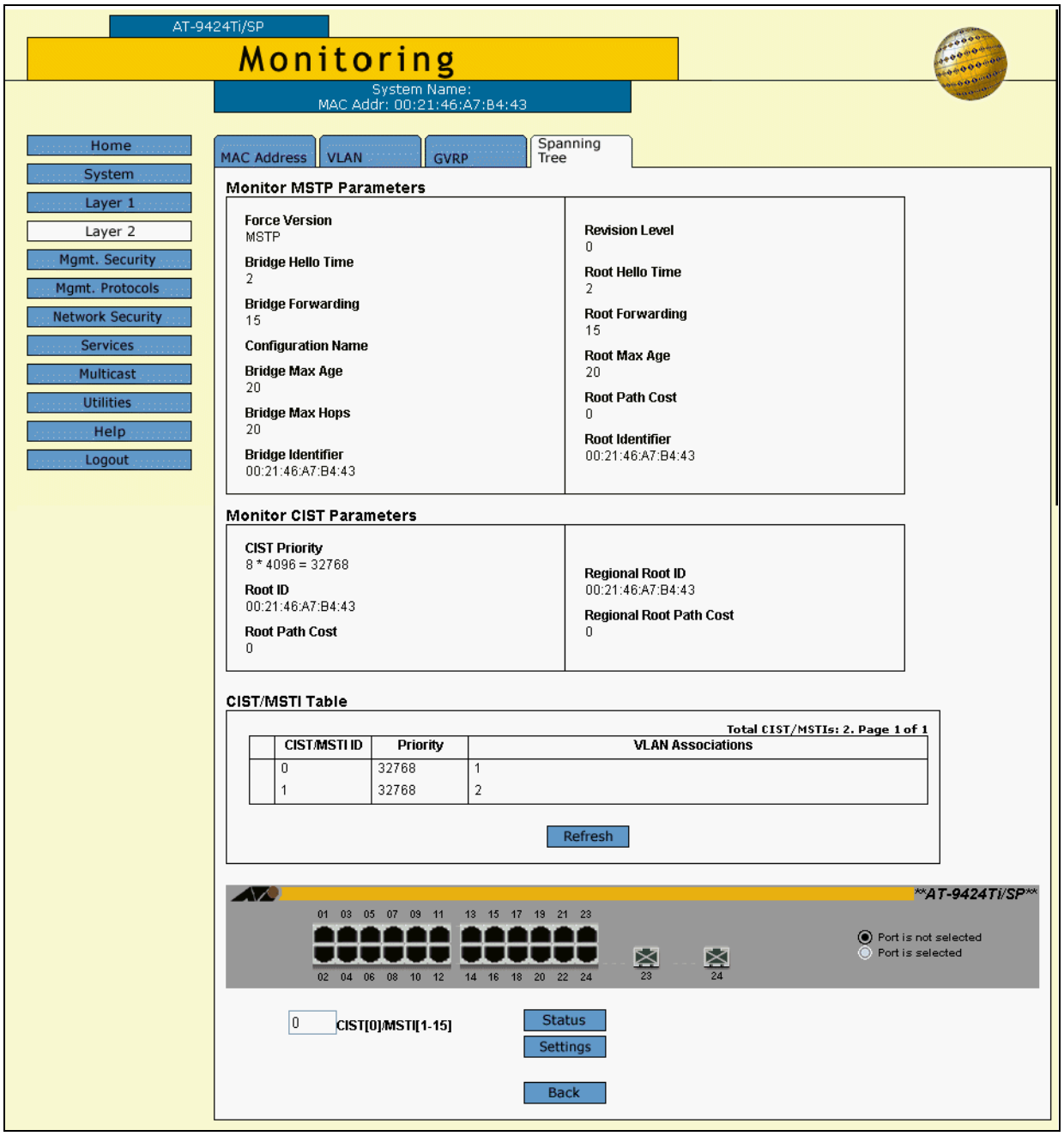

Figure 125. Monitor MSTP Parameters Tab (Monitoring)

The Monitor MSTP Parameters section displays the current MSTP parameter settings and the settings for the same parameters from the root bridge of the spanning tree domain. For definitions of the parameters, refer to "Configuring MSTP Parameters" on page 296.

5. To view MSTP port settings or status, click a port. You can select more than one port.

6. In the CIST/MSTI field, specify the MSTI where the port is a member through its VLAN assignment. You can specify only one value. The default is 0 for CIST.

7. Click **Settings** or **Status**.

   The MSTP Settings - Port (s) page is shown in Figure 126.

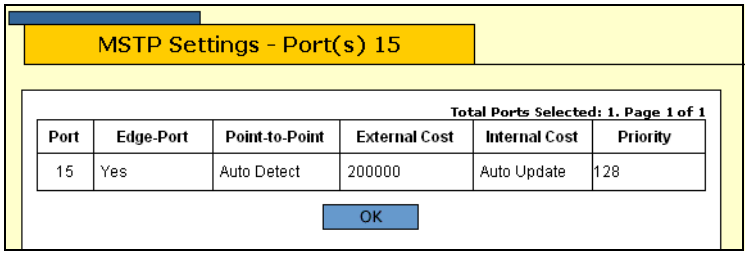

Figure 126. MSTP Settings - Port(s) Page

The MSTP Settings page displays a table that contains the following columns of information:

Port
The port number.

Edge-Port
Whether the port is functioning as an edge port. The possible settings are Yes and No.

Point-to-Point
Whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

External Cost
The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP.

Internal Cost
The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. If the setting is Auto Update, the port cost is set automatically depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge.

The MSTP Port Status - Port(s) page is shown in Figure 127.

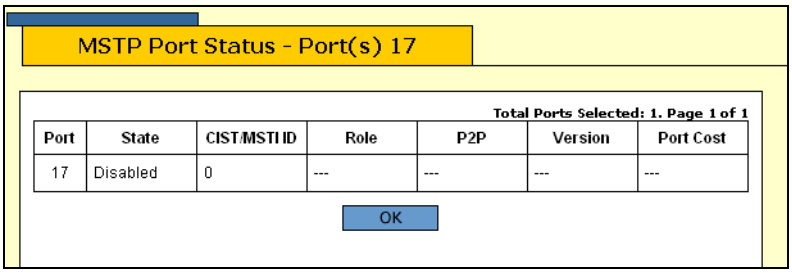

Figure 127. MSTP Port Status - Port(s) Page

The MSTP Port Status page displays a table with the following columns of information:

Port
The port number.

State
The MSTP state of the port. The possible states are:

Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission.

Learning - The port is enabled for receiving, but not forwarding packets.

Forwarding - Normal operation.

Disabled - The port has not established a link with its end node.

Role
The MSTP role of the port. The possible roles are:

Root - The port that is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path in the direction of the root switch.

Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called "master" when the CIST role is "root."

P2P
Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

Version
Whether the port is operating in MSTP mode or STP-compatible mode.

Internal Port Cost
The port cost when the port is connected to a bridge in the same MSTP region.

8. Click **OK** to close the page.

Resetting MSTP to the Default Settings

To reset MSTP to the factory default settings, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **Spanning Tree** tab.

   The Spanning Tree tab is shown in Figure 120 on page 294.
4. Click **Configure**.

   The expanded MSTP Spanning Tree tab is shown in Figure 121 on page 297.
5. Click **Defaults**.

   The MSTP settings are returned to their default values.
6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Section V

Virtual LANs

This section has the following chapters:

- Chapter 20, “Port-based and Tagged VLANs” on page 317
- Chapter 21, “GARP VLAN Registration Protocol” on page 331

Chapter 20

Port-based and Tagged VLANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs. This chapter also explains how to select a multiple VLAN mode.

This chapter contains the following sections:

- ❒ “Creating a New Port-Based or Tagged VLAN” on page 318
- ❒ “Modifying a VLAN” on page 323
- ❒ “Deleting a VLAN” on page 325
- ❒ “Selecting a VLAN Mode” on page 326
- ❒ “Displaying VLANs” on page 327

Creating a New Port-Based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 128.

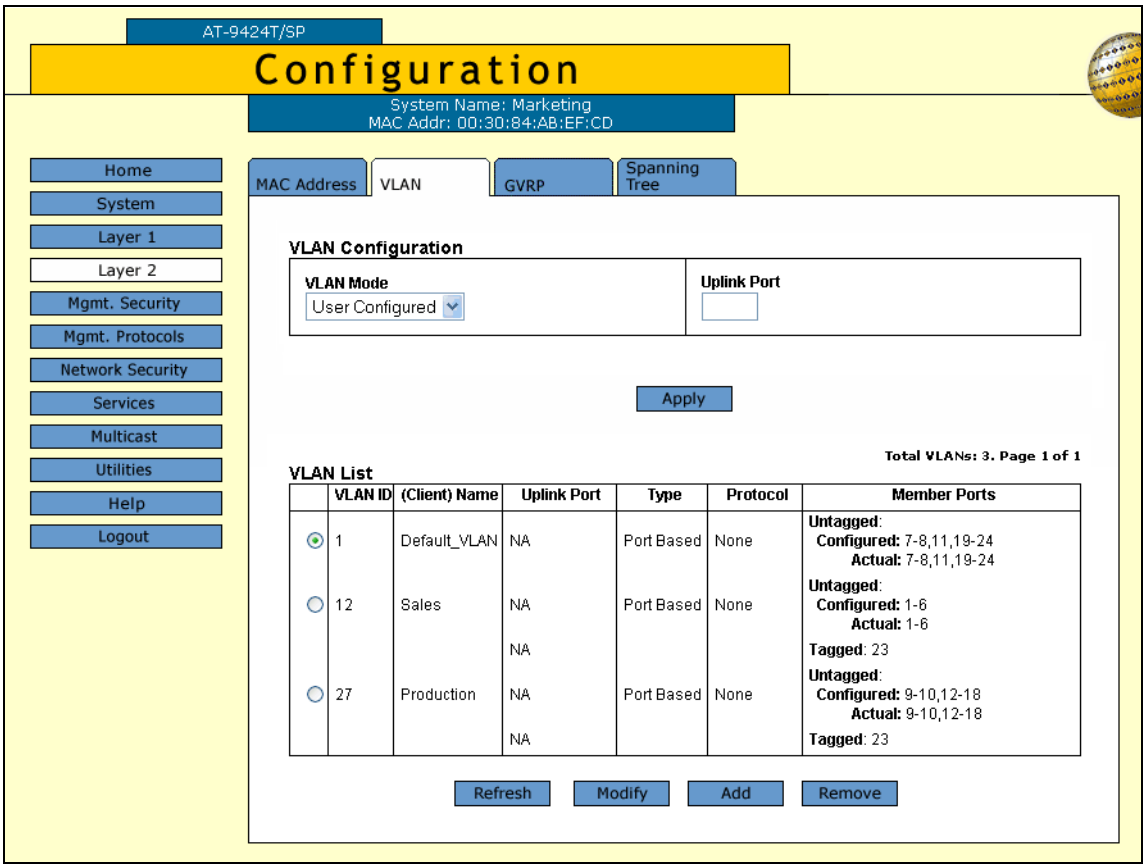

Figure 128. VLAN Tab (Configuration)

Note
The Modify and Remove buttons are not shown in the tab if the only VLAN on the switch is the Default_VLAN.

The VLAN Mode and Uplink Port options are explained in “Selecting a VLAN Mode” on page 326.

The VLAN List section displays the current VLANs on the switch and contains the following columns of information:

VID ID
The VLAN ID.

(Client) Name
The name of the VLAN.

Uplink Port
This column contains "NA," meaning Not Applicable, for tagged, port-based, and MAC address-based VLANs. For a protected ports VLAN, this column contains the uplink port(s) for a port group. Tagged uplink ports are designated with "T" and untagged uplink ports with "U." If the switch is operating in one of the two multiple VLAN modes this column displays the uplink port for the ports on the switch.

Type
The VLAN type. The possible settings are:

Port Based - The VLAN is a port-based or tagged VLAN.

MAC Based - The VLAN is a MAC address-based VLAN.

Protected - The VLAN is a protected ports VLAN.

GARP - The VLAN was automatically created by GARP.

Protocol
The protocol associated with a VLAN. The possible settings are:

None - The VLAN is a port-based, tagged, MAC address-based, or protected ports VLAN.

GARP - The VLAN was created by GARP.

Member Ports
The untagged and tagged ports of a VLAN. (These fields will be blank for a MAC address-based VLAN.) The untagged ports of a VLAN are listed as follows.

- Configured: The untagged ports assigned to the VLAN when the VLAN was created or modified.
- Actual: The current untagged ports of the VLAN. If you are not using 802.1x Port-based Network Access Control, both the Configured and Actual untagged ports of a VLAN will always be the same.

  If you are using 802.1x and assigned a Guest VLAN to an authenticator port or associated an 802.1x supplicant to a VLAN on the authentication server, a port can be in different VLAN than the virtual LAN where it was originally assigned as an untagged port. In these situations, the Configured and Actual port lists can differ, with the Actual list detailing the ports that are currently functioning as

untagged ports of the VLAN.

For example, if a particular port is listed as a Configured member of a VLAN, but not as an Actual member, that would mean either the port is currently a part of a Guest VLAN or the supplicant who logged on the port was associated with a VLAN assignment on the authentication server.

4. To add a new VLAN, click **Add**.

   The Add New VLAN page is shown in Figure 129.

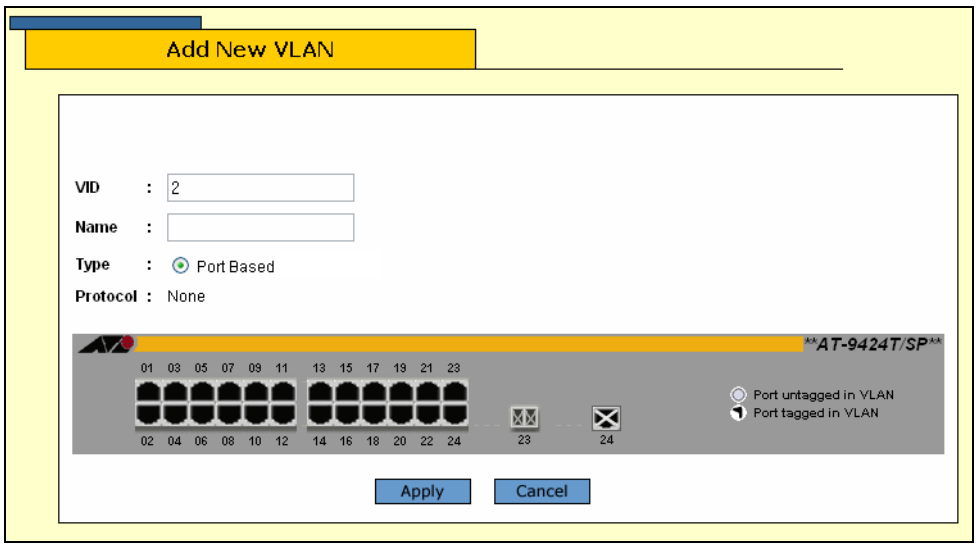

Figure 129. Add New VLAN Page

5. Configure the following parameters as necessary.

   VID
   Enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

   If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you should assign the Sales VLAN on each switch the same VID value.

   Note
   A VLAN must have a VID.

   The switch is only aware of the VIDs of the VLANs on the device and not those already being used in the network. For example, if you add a new AT-9400 Series switch to a network where the existing VLANs

use VIDs 2 through 24, the default VID value for the first VLAN created on the switch is still VID 2, even though that number is already being used. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Name
Specify a name for the new VLAN.

The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that are part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

If the VLAN is unique in your network, then the name should be unique as well. If the VLAN is part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

Note
A VLAN must be assigned a name.

Type
Select **Port Based** as the Type to create a port-based or tagged VLAN. This is the only option.

Note
You must use the menus or command line interface to create a MAC address-based VLAN or protected ports VLAN.

6. To select the VLAN ports, click on the ports in the switch image. Clicking repeatedly on a port toggles it through the following settings:

   Untagged port

   Tagged port

   Not a member of the VLAN

7. Click **Apply**. The new user-configured VLAN is now ready for network operations.

Note
Untagged ports assigned to the new VLAN are automatically removed from their current untagged VLAN assignment.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying a VLAN

This procedure explains how to add or remove ports from a tagged or untagged VLAN. When modifying a VLAN, note the following:

- You cannot change the VID of a VLAN.
- You cannot change the name of a VLAN using the web browser interface, but you can from the menus or command line interface.
- You cannot modify VLANs when the switch is operating in one of the multiple VLAN modes.
- You cannot modify a protected posts VLAN or a MAC address-based VLAN from the web browser interface.
- If the switch is using 802.1x Port-based Network Access Control and you want to move an untagged port to a different VLAN, the port's 802.1x role must be set to none. You cannot move an untagged port to a different VLAN while the port is functioning as an 802.1x authenticator or supplicant port. For instructions on how to change a port's 802.1x role, refer to "Setting Port Roles" on page 354.

To modify a VLAN, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 128 on page 318.
4. Click the button next to the name of the VLAN to be modified.
5. Click **Modify**.

   The Modify VLAN page for the VLAN is displayed.
6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image. Clicking repeatedly on a port toggles the port through the following possible settings:

   Untagged port

   Tagged port

   Port is not a member of the VLAN
7. Click **Apply**.

Note
Untagged ports added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN leaves the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting a VLAN

This procedure deletes port-based and tagged VLANs from the switch. Note the following before performing this procedure:

- You cannot delete the Default_VLAN.
- You cannot delete a VLAN if it has a routing interface. You must delete the routing interface first. Deleting an interface is not supported from the web browser interface. That management function must be performed from the menus or command line interface.
- All untagged ports in a deleted VLAN are returned to the Default_VLAN as untagged ports.
- Static addresses assigned to the ports of a deleted VLAN become obsolete and should be deleted from the MAC address table. For instructions, refer to "Deleting Unicast and Multicast MAC Addresses" on page 81.
- If the switch is part of an enhanced stack, deleting the common VLAN that interconnects the switch with the stack removes the switch from the stack.

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 128 on page 318.
4. Click the button next to the name of the VLAN to be deleted. (You cannot delete the Default_VLAN.)
5. Click **Remove**.

   A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Selecting a VLAN Mode

The AT-S63 Management Software features three VLAN modes:

- Port-based and tagged VLAN Mode (default mode)
- IEEE 802.1Q-compliant Multiple VLAN Mode
- Non-IEEE 802.1Q compliant Multiple VLAN Mode

For background information, refer to the *AT-S63 Management Software Features Guide*.

Note
Any existing port-based or tagged VLANs are not retained when you change the VLAN mode from the user configured mode to a multiple VLAN mode and, at some point, reset the switch. The user configured VLAN information is lost and you must recreate the information if you later return the switch to the user configured VLAN mode.

To select a VLAN mode for the switch, perform the procedure below:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **VLAN** tab. The VLAN tab is shown in Figure 128 on page 318.
4. In the VLAN Mode section, select a VLAN mode. Only one mode can be active on the switch at a time. The modes are:

   User Configured - Port-based and tagged VLAN Mode

   Multiple - Non-IEEE 802.1Q-compliant Multiple VLAN Mode

   Multiple 802.1Q - IEEE 802.1Q-compliant Multiple VLAN Mode
5. If you are selecting one of the multiple VLAN modes, specify an uplink port in the Uplink Port field. This port functions as the uplink port for the VLANs. The default is port 1.
6. Click **Apply**. The new mode is automatically activated on the switch.
7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying VLANs

To display the current VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **VLAN** tab.

   The VLAN tab is shown in Figure 130.

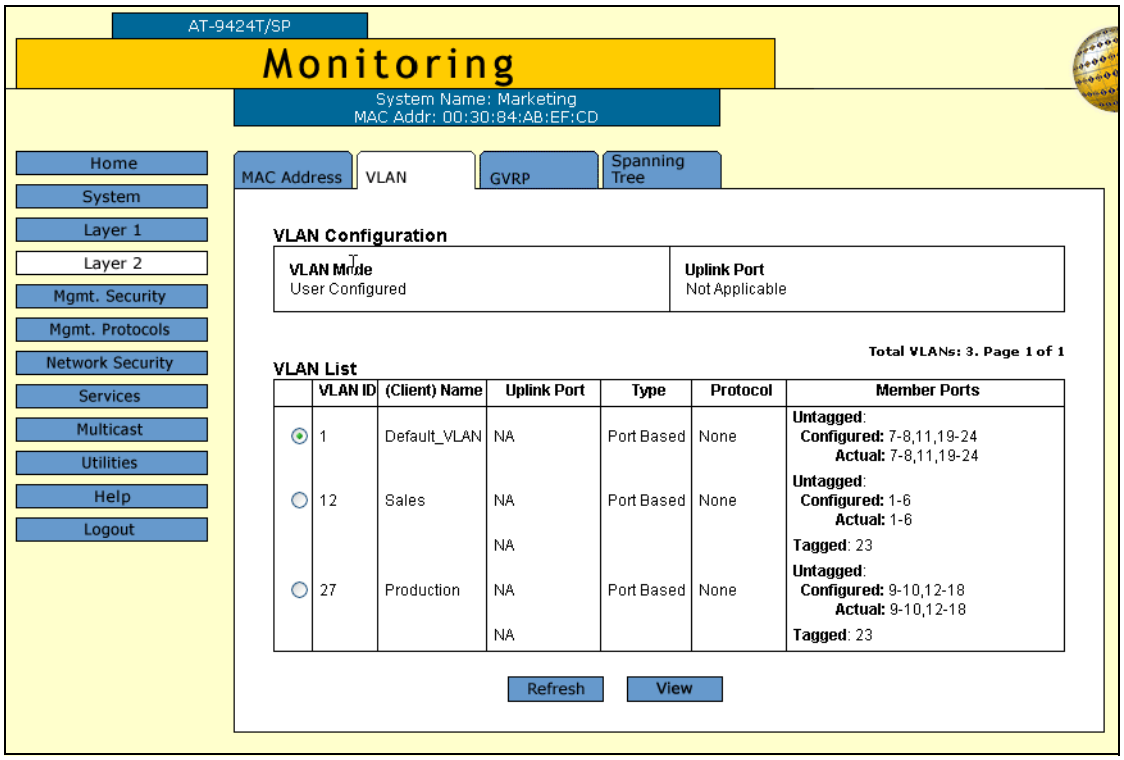

Figure 130. VLAN Tab (Monitoring)

The upper part of the tab displays the following information:

VLAN Mode
The VLAN mode of the switch. Possible settings are:

User Configured - This mode supports port-based and tagged VLANs.

Multiple 802.1Q - The IEEE 802.1Q-compliant multiple VLAN mode.

Multiple - The non-IEEE 802.1Q-compliant multiple VLAN mode.

Uplink Port
This item only applies when the switch is operating in the IEEE 802.1Q-compliant multiple VLAN mode or the non-IEEE 802.1Q-compliant multiple VLAN modes. It displays the uplink port for the VLANs.

The lower part of the tab displays a table that contains the following columns of information:

VLAN ID
The VID number of the VLAN.

(Client) Name
The name of the VLAN. If the switch is operating in one of the multiple VLAN modes, the names of the VLANs start with “Client,” with the exception of the VLAN containing the uplink port, which starts with “Uplink.”

Uplink Port
This column contains “NA,” meaning Not Applicable, for tagged, port-based, and MAC address-based VLANs. For a protected ports VLAN, this column contains the uplink port(s) for a port group. Tagged uplink ports are designated with “T” and untagged uplink ports with “U.” If the switch is operating in one of the two multiple VLAN modes this column displays the uplink port for the ports on the switch.

Type
The VLAN type. The possible settings are:

Port Based - The VLAN is a port-based or tagged VLAN.

MAC Based - The VLAN is a MAC address-based VLAN.

Protected - The VLAN is a protected ports VLAN.

GARP - The VLAN was created by GARP.

Protocol
The protocol associated with this VLAN. The possible settings are:

Blank - The VLAN is a port-based, tagged, protected port, or MAC address-based VLAN.

GARP - The VLAN is a dynamic GVRP VLAN or the port is a dynamic GVRP port of a static VLAN.

Member Ports
The untagged and tagged ports of a VLAN. (These fields will be blank for a MAC address-based VLAN.) The untagged ports of a VLAN are listed as follows.

- Configured: The untagged ports assigned to the VLAN when the VLAN was created or modified.

- Actual: The current untagged ports of the VLAN. If you are not using 802.1x Port-based Network Access Control, both the Configured and Actual untagged ports of a VLAN will always be the same.

  If you are using 802.1x and you assigned a Guest VLAN to an authenticator port or you associated an 802.1x supplicant to a VLAN on the authentication server, a port can be in different VLAN than the virtual LAN where it was originally assigned as an untagged port. In these situations, the Configured and Actual port lists can differ, with the Actual list detailing the ports that are currently functioning as untagged ports of the VLAN.

  For example, if a port is listed as a Configured member of a VLAN, but not as an Actual member, that would mean either the port is currently a part of a Guest VLAN or the supplicant who logged on the port was associated with a VLAN assignment on the authentication server.

4. To display the groups of a protected ports VLAN, click the circle next to the VLAN and click **View**.

   The View Protected VLAN page is shown in Figure 131.

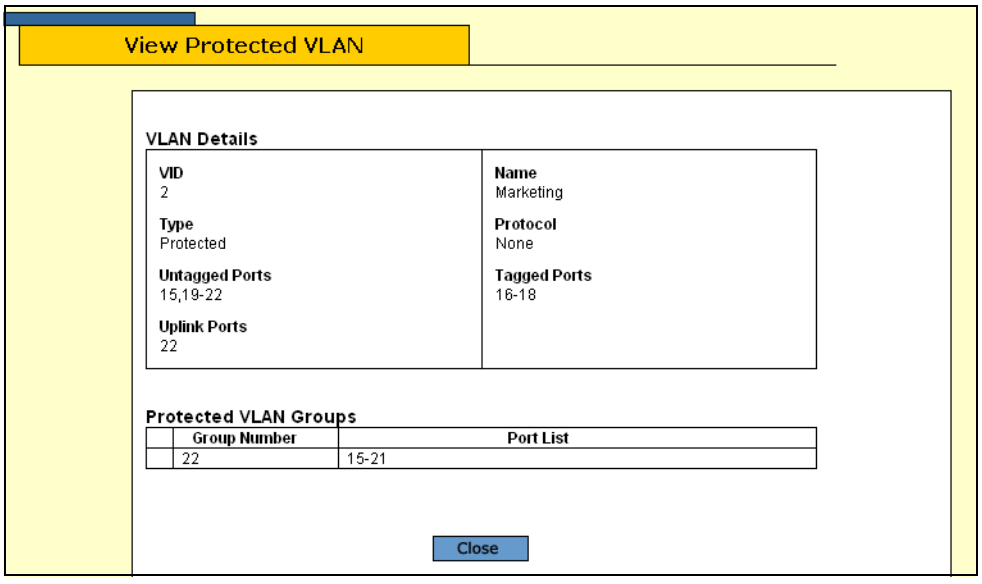

Figure 131. View Protected VLAN Page

The VLAN Details section displays the following information.

VID
The VLAN ID.

Type
The VLAN type which is always Protected.

Untagged Ports
The untagged ports members of the VLAN.

Uplink Ports
The uplink port(s) for this group of ports.

Name
The VLAN name.

Protocol
Not used.

Tagged Ports
The tagged ports members of the VLAN.

The Protected VLAN Groups section displays the following information:

Group Number
The number assigned to the group.

Port List
The ports of the group.

Chapter 21

GARP VLAN Registration Protocol

This chapter contains instructions on how to configure GARP VLAN Registration Protocol (GVRP). This chapter contains the following procedures:

- ❒ “Configuring GVRP” on page 332
- ❒ “Enabling or Disabling GVRP on a Port” on page 334
- ❒ “Displaying the GVRP Configuration” on page 335
- ❒ “Displaying the GVRP Port Configuration” on page 336
- ❒ “Displaying the GVRP Database” on page 337
- ❒ “Displaying the GVRP State Machine” on page 338
- ❒ “Displaying the GVRP Counters” on page 341
- ❒ “Displaying the GIP Connected Ports Ring” on page 344

Configuring GVRP

To configure GVRP, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 132.

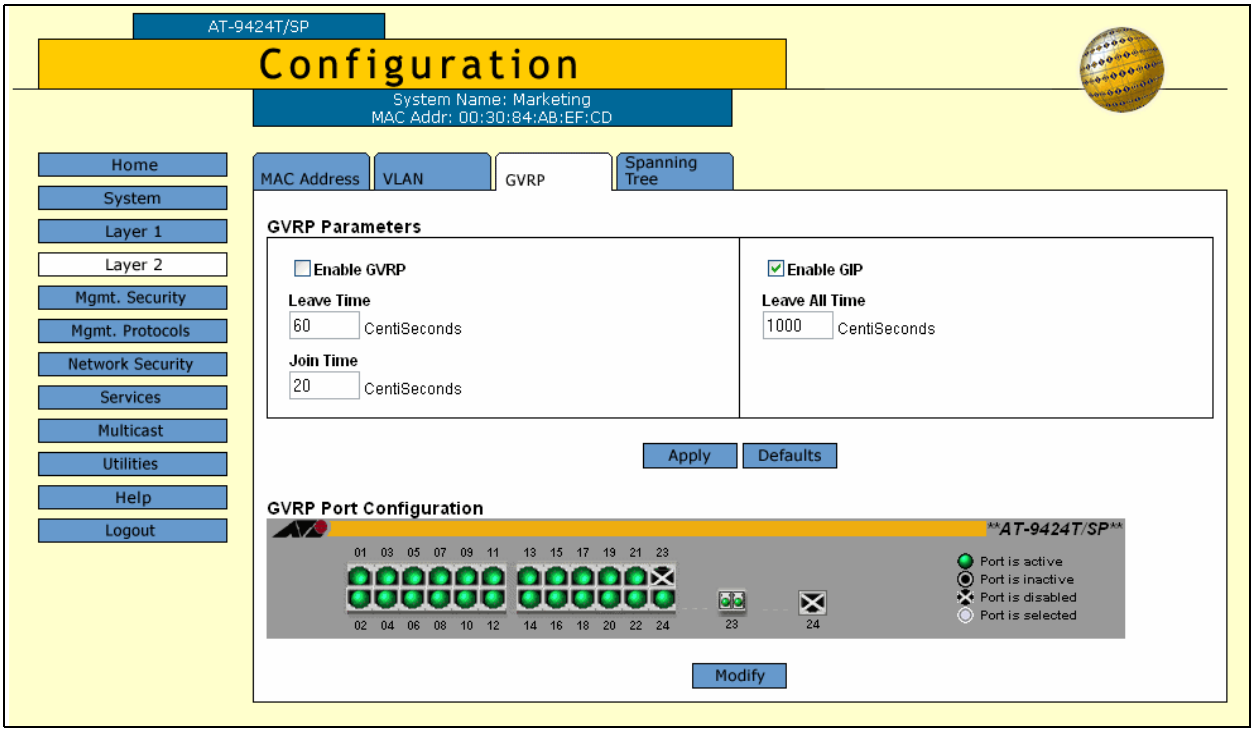

Figure 132. GVRP Tab (Configuration)

4. In the GVRP Parameters section, configure the following parameters as necessary.

Note
The settings for the three timers must be the same on all GVRP-active network devices.

Enable GVRP
Click to enable or disable GVRP.

Leave Time
Use this parameter to specify the leave time. The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time
Use this parameter to specify the join time. The range is 10 to 60 centiseconds and the default is 20 centiseconds. This parameter must be in relation to the GVRP Leave Timer according to the following equation:

Join Timer <= (2 x (GVRP Leave Timer))

Enable GIP
Click to enable GIP, which is required to propagate VLAN information among the ports of the switch.

Leave All Time
The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

5. Click **Apply**.

   Configuration changes are immediately activated on the switch.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Enabling or Disabling GVRP on a Port

To enable or disable GVRP on a port, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 132 on page 332.
4. In the GVRP Port Configuration section, click the ports to be to configured.
5. Click **Modify**.

   The GVRP Port Configuration page is shown in Figure 133.

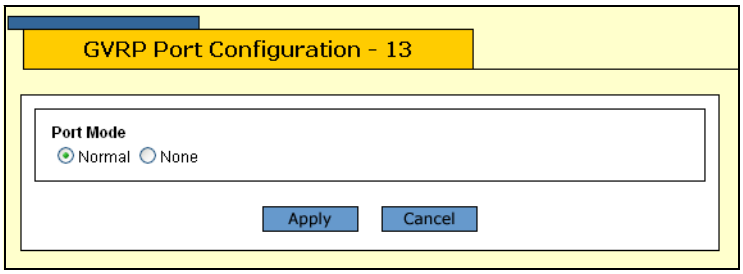

Figure 133. GVRP Port Configuration Page

6. Click **Normal** to have the port propagate GVRP information, or **None** to prevent processing GVRP information and transmitting PDUs.
7. Click **Apply** to activate the change, or **Cancel** to cancel.
8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the GVRP Configuration

To display the GVRP configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134.

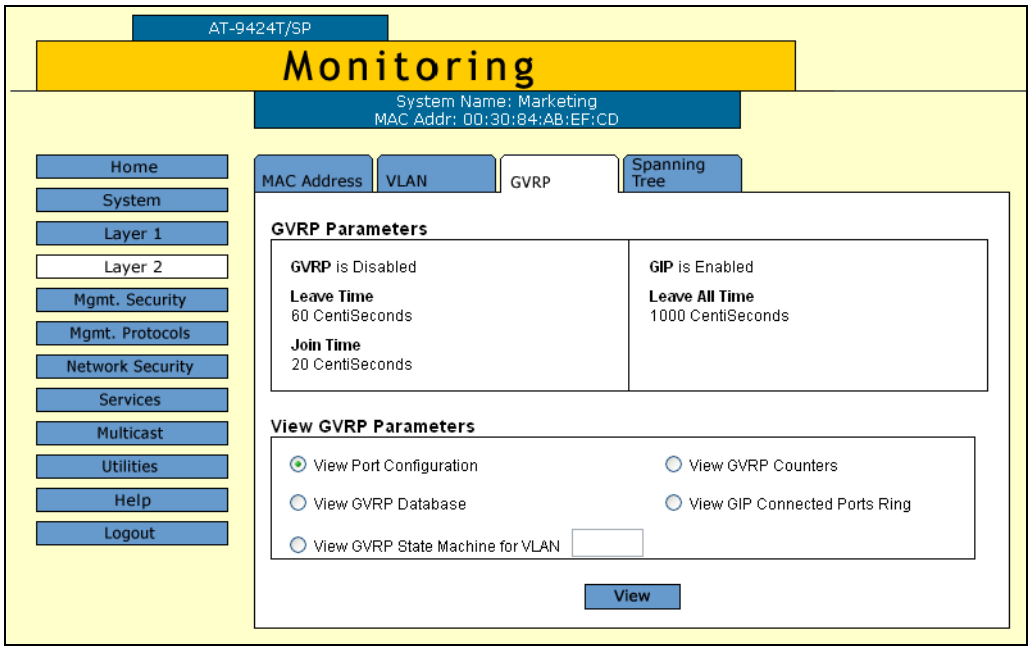

Figure 134. GVRP Tab (Monitoring)

The GVRP Parameters section provides the following information:

GVRP
The GVRP status, Enabled or Disabled.

Leave Time
The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time
The range is 10 to 60 centiseconds and the default is 20 centiseconds.

GIP
The GIP status, Enabled or Disabled.

Leave All Time
The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

Displaying the GVRP Port Configuration

To display the GVRP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134 on page 335.
4. In the View GVRP Parameters section, click **View Port Configuration**.
5. Click **View**.

   The GVRP Port Configuration page is shown in Figure 135.

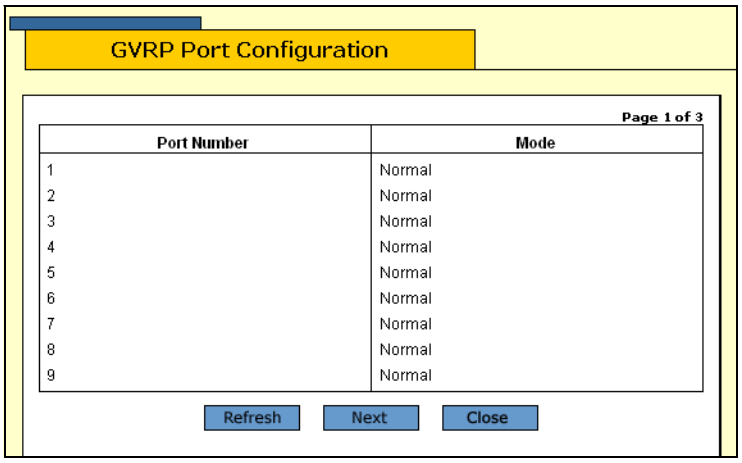

Figure 135. GVRP Port Configuration Page

The GVRP Port Configuration page provides the following information:

Port Number
The port number.

Mode
The port mode, either Normal or None.

Displaying the GVRP Database

To display the GVRP database, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134 on page 335.
4. In the View GVRP Parameters section, click **View GVRP Database**.
5. Click **View**.

   The GVRP Database page is shown in Figure 136.

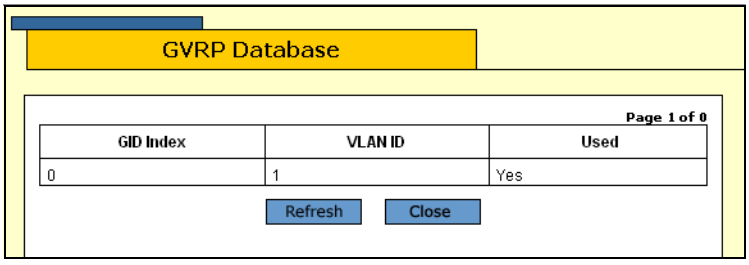

Figure 136. GVRP Database Page

The GVRP Database page provides the following information:

GID Index
The value of the GID index corresponding to the attribute.

VLAN ID
The value of the attribute.

Used
Whether the GID index is currently being used by any port in the GARP application.

Displaying the GVRP State Machine

To display the GVRP state machine, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134 on page 335.
4. In the View GVRP Parameters section, click **View GVRP State Machine for VLAN** and enter the VLAN number in the box.
5. Click **View**.

   The GVRP State Machine for VLAN page is shown in Figure 137.

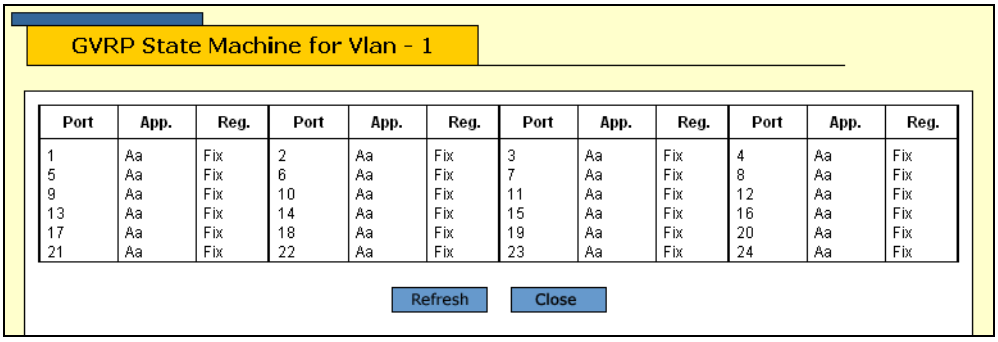
GVRP State Machine for Vlan - 1
Port App. Reg. Port App. Reg. Port App. Reg. Port App. Reg.
1 Aa Fix 2 Aa Fix 3 Aa Fix 4 Aa Fix
5 Aa Fix 6 Aa Fix 7 Aa Fix 8 Aa Fix
9 Aa Fix 10 Aa Fix 11 Aa Fix 12 Aa Fix
13 Aa Fix 14 Aa Fix 15 Aa Fix 16 Aa Fix
17 Aa Fix 18 Aa Fix 19 Aa Fix 20 Aa Fix
21 Aa Fix 22 Aa Fix 23 Aa Fix 24 Aa Fix
Refresh
Close

Figure 137. GVRP State Machine for VLAN Page

The GVRP State Machine for VLAN page provides the information shown in Table 11.

Table 11. GVRP State Machine Parameters

Parameter	Meaning
Port	Port number on the switch; this port belongs to the GARP application. If the GARP application has no ports, “No ports have been assigned” is displayed.

Table 11. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
App	Applicant state machine for the GID index on that particular port. One of:	
	Normal Participant Management state:	
	"Vo"	Very Anxious Observer
	"Ao"	Anxious Observer
	"Qo"	Quiet Observer
	"Lo"	Leaving Observer
	"Vp"	Very Anxious Passive Member
	"Ap"	Anxious Passive Member
	"Qp"	Quiet Passive Member
	"Va"	Very Anxious Active Member
	"Aa"	Anxious Active Member
	"Qa"	Quiet Active Member
	"La"	Leaving Active Member
App (*Continued*)	*Non-Participant Management state:*	
	"Von"	Very Anxious Observer
	"Aon"	Anxious Observer
	"Qon"	Quiet Observer
	"Lon"	Leaving Observer
	"Vpn"	Very Anxious Passive Member
	"Apn"	Anxious Passive Member
	"Qpn"	Quiet Passive Member
	"Van"	Very Anxious Active Member
	"Aan"	Anxious Active Member
	"Qan"	Quiet Active Member
	"Lan"	Leaving Active Member
	The initialized state for the Applicant is Vo.	

Table 11. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
Reg	Registrar state machine for the GID index on that particular port. One of:	
	“Mt”	Empty
	“Lv3”	Leaving substate 3 (final Leaving substate)
	“Lv2”	Leaving substate 2
	“Lv1”	Leaving substate 1
	“Lv”	Leaving substate (initial Leaving substate)
	“In”	In
	“Fix”	Registration Fixed
	“For”	Registration Forbidden
	The initialized state for the Registrar is Mt.	

Displaying the GVRP Counters

To display the GVRP counters, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134 on page 335.
4. In the View GVRP Parameters section, click **View GVRP Counters**.
5. Click **View**.

   The GVRP Counters page is shown in Figure 138.

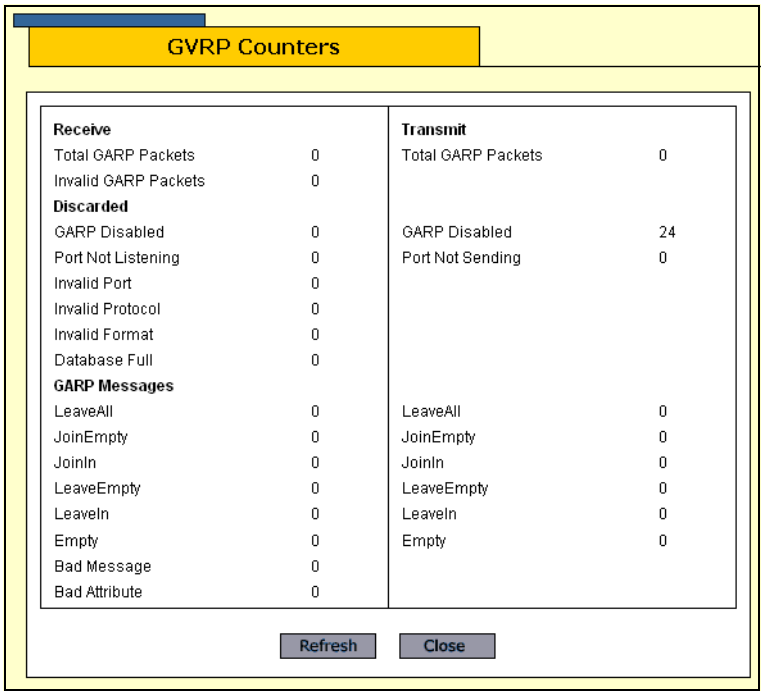

Figure 138. GVRP Counters Page

The GVRP Counters page provides the information shown in Table 12.

Table 12. GVRP Counters

Parameter	Meaning
Receive: Total GARP Packets	Total number of GARP PDUs received by this GARP application.

Table 12. GVRP Counters (Continued)

Parameter	Meaning
Transmit: Total GARP Packets	Total number of GARP PDUs transmitted by this GARP application.
Receive: Invalid GARP Packets	Number of invalid GARP PDUs received by this GARP application.
Receive Discarded: GARP Disabled	Number of received GARP PDUs discarded because the GARP application was disabled.
Transmit Discarded: GARP Disabled	Number of GARP PDUs discarded because the GARP application was disabled. This counter is incremented when ports are added to or deleted from the GARP application arising from port movements in the underlying VLAN or STP.
Receive Discarded: Port Not Listening	Number of GARP PDUs discarded because the port that received the PDUs was not listening, that is, MODE=NONE was set on the port.
Transmit Discarded: Port Not Sending	Number of GARP PDUs discarded because the port that the PDUs were to be transmitted on was not sending, that is, MODE=NONE was set on the port.
Receive Discarded: Invalid Port	Number of GARP PDUs discarded because the port that received the PDU does not belong to the GARP application.
Receive Discarded: Invalid Protocol	Number of GARP PDUs discarded because the GARP PDU contained an invalid protocol.
Receive Discarded: Invalid Format	Number of GARP PDUs discarded because the format of the GARP PDU was not recognized.
Receive Discarded: Database Full	Number of GARP PDUs discarded because the database for the GARP application was full, that is, the maximum number of attributes for the GARP application is in use.
Receive GARP Messages: LeaveAll	Number of GARP LeaveAll messages received by the GARP application.
Transmit: GARP Messages: LeaveAll	Number of GARP LeaveAll messages transmitted by the GARP application.
Receive GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages received for all attributes in the GARP application.

Table 12. GVRP Counters (Continued)

Parameter	Meaning
Transmit GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: JoinIn	Total number of GARP JoinIn messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinIn	Total number of GARP JoinIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveIn	Total number of GARP LeaveIn messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveIn	Total number of GARP LeaveIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Empty	Total number of GARP Empty messages received for all attributes in the GARP application.
Transmit GARP Messages: Empty	Total number of GARP Empty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Bad Message	Number of GARP messages that had an invalid Attribute Type value, an invalid Attribute Length value or an invalid Attribute Event value.
Receive GARP Messages: Bad Attribute	Number of GARP messages that had an invalid Attribute Value value.

Displaying the GIP Connected Ports Ring

To display the GIP connected ports ring, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Layer 2** option.
3. Select the **GVRP** tab.

   The GVRP tab is shown in Figure 134 on page 335.
4. In the View GVRP Parameters section, click **View GIP Connected Ports Ring**.
5. Click **View**.

   The GIP Connected Ports Ring page is shown in Figure 139.

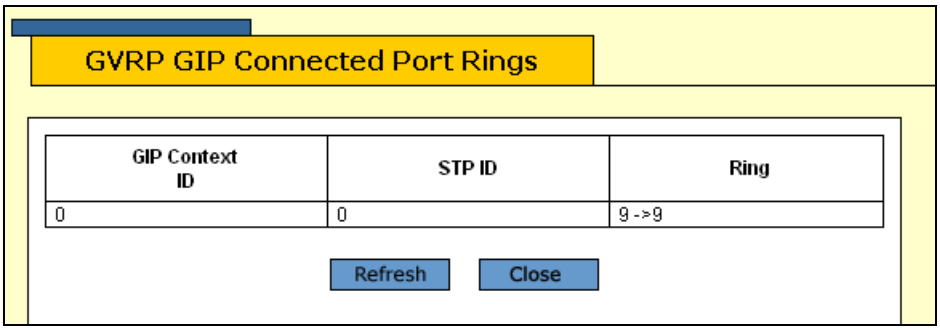

Figure 139. GIP Connected Ports Ring Page

The GIP Connected Ports Ring page displays a table that contains the following columns of information:

GIP Context ID
A number assigned to the instance for the GIP context.

STP ID
Present if the GARP application is GVRP; identifies the spanning tree instance associated with the GIP context.

Ring
The ring of connected ports. Only ports presently in the spanning tree Forwarding state are eligible for membership in the GIP connected ring. If no ports exist in the GIP connected ring, “No ports are connected” is displayed. If the GARP application has no ports, “No ports have been assigned” is displayed.

Section VI

Port Security

This section has the following chapters:

- Chapter 22, “MAC Address-based Port Security” on page 347
- Chapter 23, “802.1x Port-based Network Access Control” on page 353

Chapter 22

MAC Address-based Port Security

This chapter explains how to configure and display the MAC address-based security levels on the ports on the switch. It contains the following sections:

- ❒ “Configuring Port Security” on page 348
- ❒ “Displaying Port Security Levels” on page 351

Configuring Port Security

To configure security for the ports, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.

   The Network Security page opens with the Port Security tab selected by default, as shown in Figure 140.

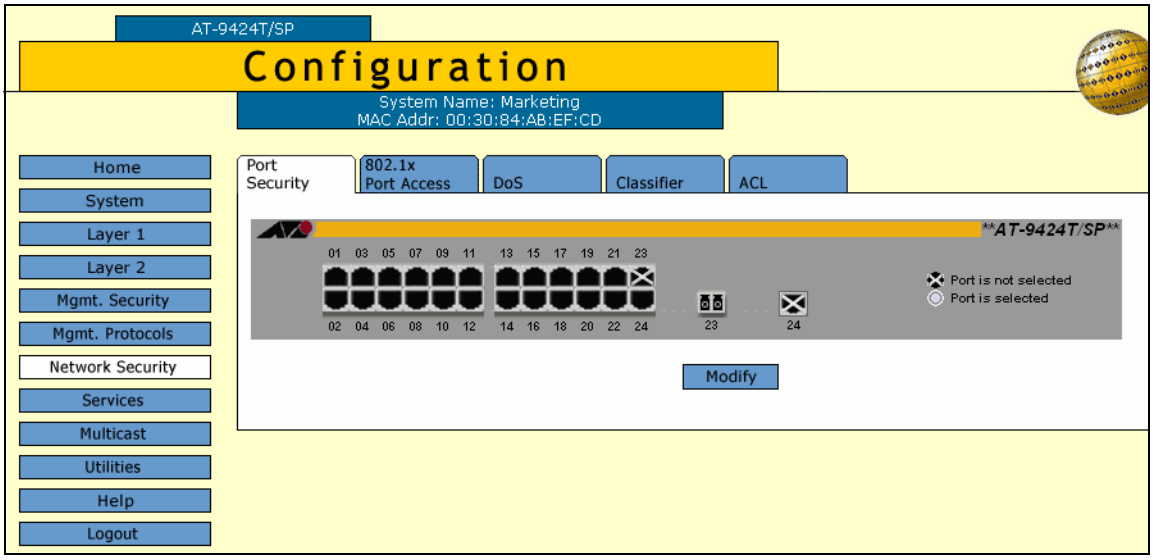

Figure 140. Port Security Tab (Configuration)

3. In the image of the switch, click the port to be configured and click **Modify**. A selected port turns white. You can configure more than one port at a time. The Security for Ports page is shown in Figure 143.

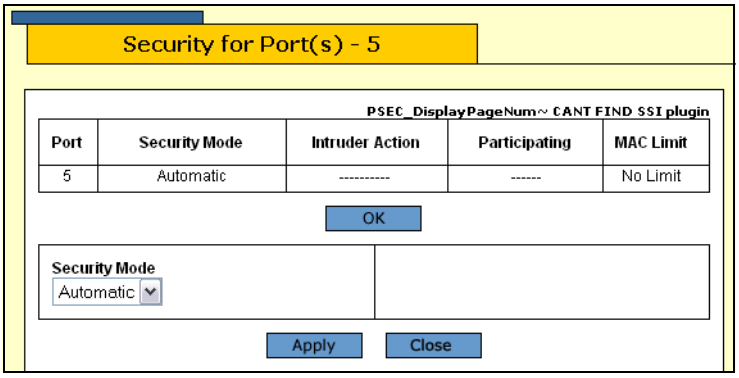

Figure 141. Security for Ports Page (Configuration)

4. From the Security Mode pull-down menu, select the desired port security level for the port. Options are:

   Automatic
   Disables MAC address-based port security on a port. This is the default setting.

   Limited
   Allows you to specify a maximum number of dynamic source MAC addresses a port can learn. After learning its maximum number of addresses, a port discards all ingress frames with source MAC addresses not already learned.

   When the Limited security mode is initially activated on a port, all dynamic MAC addresses learned by the port are deleted from the MAC address table. The port then begins to learn new addresses, up to the maximum allowed. After the port has learned its maximum number of addresses, it does not learn any new addresses, even when end nodes are inactive.

   A dynamic MAC address learned on a port operating in the Limited security mode never times out from the MAC address table, even when the corresponding end node is inactive.

   Static MAC addresses are retained by the port and are not included in the count of maximum dynamic addresses. You can continue to add static MAC addresses to a port operating with this security level, even after the port has already learned its maximum number of dynamic MAC addresses. A switch port can have up to 255 dynamic and static MAC addresses.

   Secured
   Instructs a port to forward frames using only static MAC addresses. The port does not learn any dynamic MAC addresses and deletes any dynamic addressees that it has already learned. Only those end nodes whose MAC addresses are entered as static addresses are able to forward frames through the port.

   After activating this security level, you must enter the static MAC addresses of the end nodes to be allowed to forward frames through the port.

   Locked
   Instructs a port to immediately stop learning new dynamic MAC addresses. Frames are forwarded using the dynamic MAC addresses already learned by the port has and any static MAC addresses assigned to the port.

   Dynamic MAC addresses learned by the port prior to the activation of this security level never time out from the MAC address table, even when the corresponding end nodes are inactive. The port will not learn any new dynamic addresses.

You can continue to add new static MAC addresses to a port operating under this security level.

5. If you select the Limited security level, additional options are displayed in the window for you to configure. They are defined here:

   Intrusion Action
   Specifies what the switch should do if a port receives an invalid frame. Options are

   - Discard - Discards the invalid frame.
   - Trap - Discards the invalid frame and sends an SNMP trap.
   - Discard - Discards the invalid frame, sends an SNMP trap, and disables the port.

   Threshold
   Specifies the maximum number of dynamic MAC addresses you want the port to be able to learn. The range is 1 to 256. The default is 100.

   Port Participating
   Applies only when the intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard. If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send the SNMP trap or disable the port. If you want the switch to send a trap and/or disable the port, you must sent this option to Yes.

6. Click **Apply**.

7. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying Port Security Levels

To display the MAC address-based security level of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Network Security**.

   The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 142.

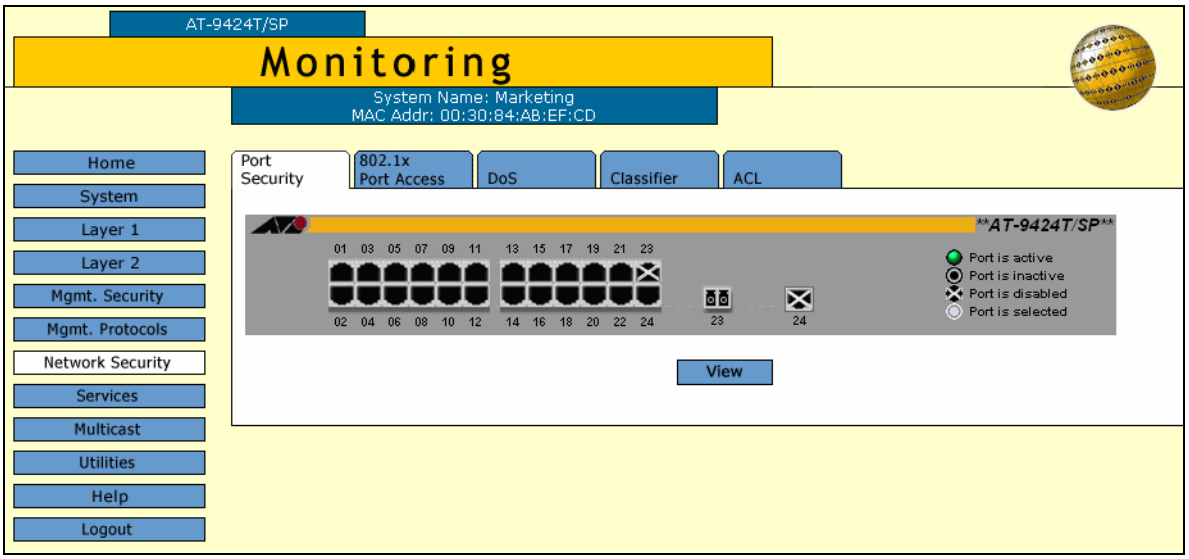

Figure 142. Port Security Tab (Monitoring)

3. Click the port whose port security level is to be displayed. A selected port turns white. You can select more than one port at a time.
4. Click **View**. The Security for Port(s) page is shown in Figure 143.

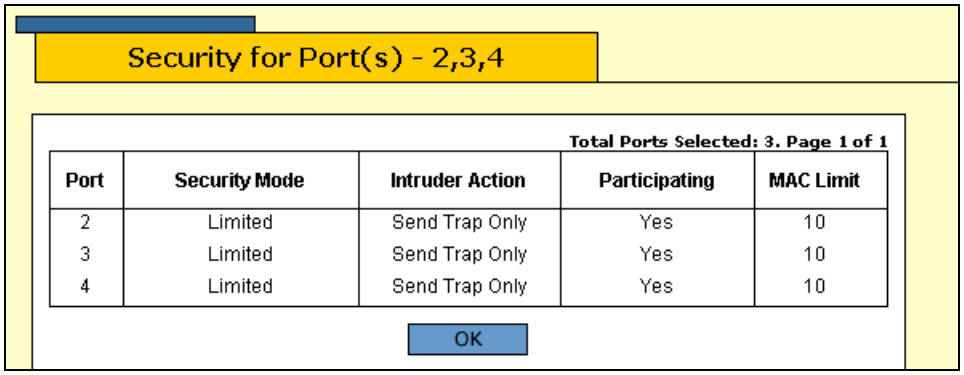

Figure 143. Security for Port(s) Page

The Security for Ports page displays a table that contains the following columns of information:

Port
The number of the port.

Security Mode
The active security mode on the port. The possible settings are Automatic, Limited, Secured, and Locked.

Intruder Action
The column specifies the action taken by the switch if a port receives an invalid packet. The possible settings are:

Discard - The port discards invalid packets. This is the default.

Trap - The port discards invalid packets and sends a trap. This action applies only to the Limited security mode.

Trap/Disable - The port discards invalid packets, sends a trap, and disables the port. This action applies only to the Limited security mode.

Note
The Participating and MAC Limit parameters only apply the Limited security level.

Participating
This column only applies when the intrusion action for a port is set to trap or disable. This option does not apply when intrusion action is set to No Action (discard). If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send a trap or disable the port.

MAC Limit
This column specifies the maximum number of dynamic MAC addresses the port learns.

Chapter 23

802.1x Port-based Network Access Control

This chapter contains instructions on how to configure the 802.1x Port-based Network Access Control feature on the switch. The chapter contains the following sections:

- ❒ “Setting Port Roles” on page 354
- ❒ “Enabling or Disabling 802.1x Port-based Network Access Control” on page 356
- ❒ “Configuring Authenticator Port Parameters” on page 357
- ❒ “Configuring Supplicant Port Parameters” on page 363
- ❒ “Displaying the Port-based Network Access Control Parameters” on page 365
- ❒ “RADIUS Accounting” on page 369

Setting Port Roles

To set port roles for port-based network access control, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 144.

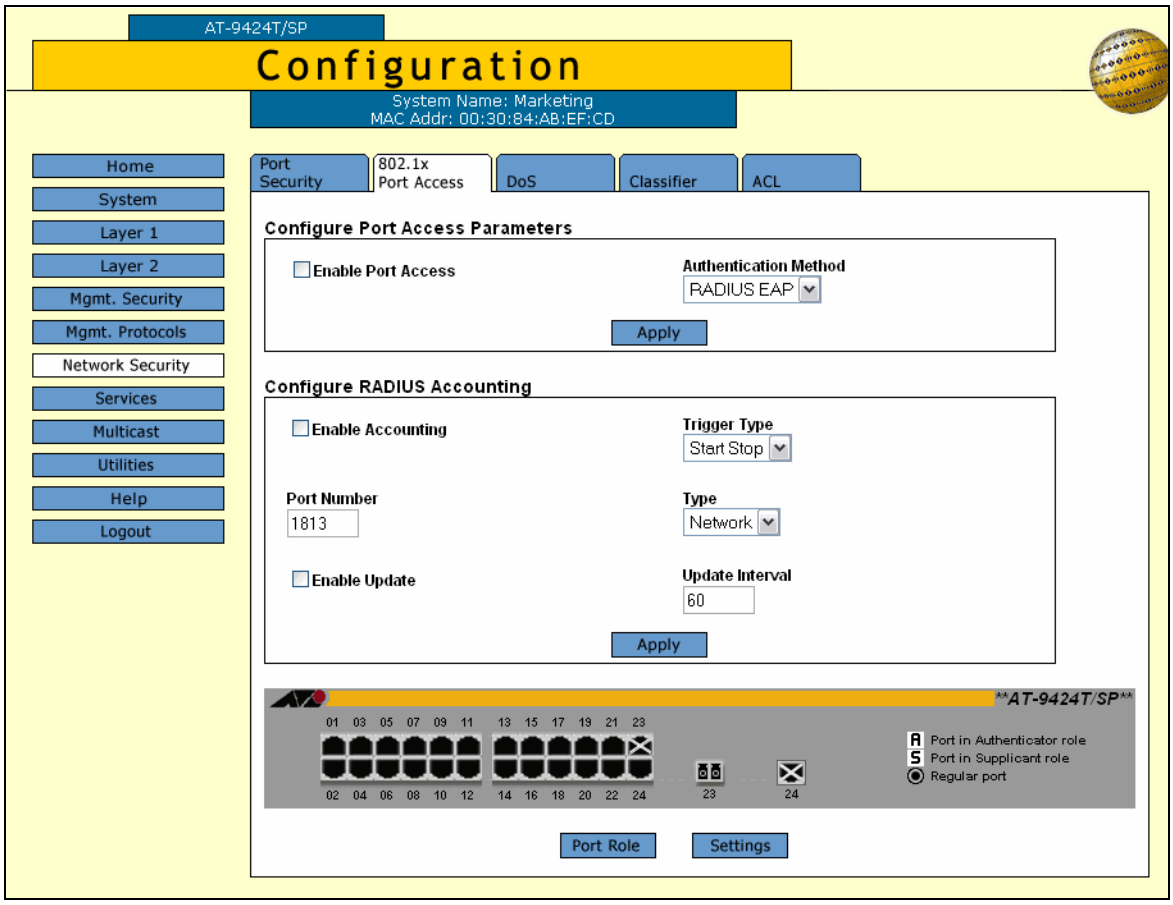

Figure 144. 802.1x Port Access Tab (Configuration)

The image of the switch displays the roles of the ports. An “A” indicates an authenticator port and an “S” a supplicant port. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.

4. To set a port’s role, click the port. A selected port turns white. You can configure more than one port at a time.

5. Click **Port Role**.

   The Port Role Configuration page is shown in Figure 145.

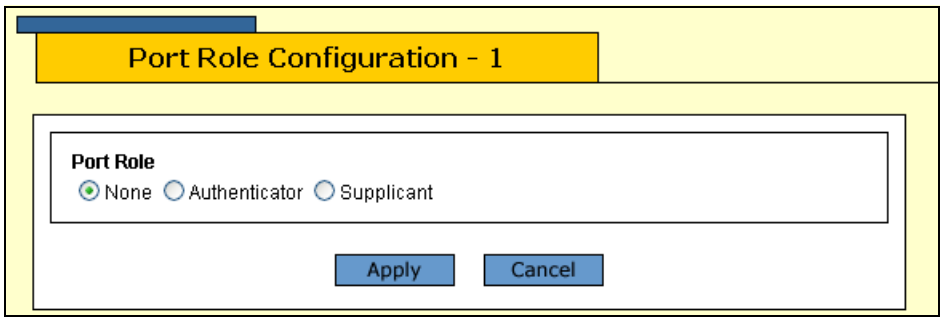

Figure 145. Port Role Configuration Page

6. Select the desired role for the port. A port can have only one port role at a time. The possible settings are:

   None
   The port does not participate in 802.1x port-based access control. This is the default setting.

   Authenticator
   The port functions as an authenticator. This is the appropriate setting if the port is connected to a supplicant.

   Supplicant
   The port functions as an supplicant. This is the appropriate setting if the port is connected to an authenticator.

7. Click **Apply**.

   The new role is immediately implemented on the port.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

   To enable or disable port-based access control, go to "Enabling or Disabling 802.1x Port-based Network Access Control" on page 356. To configure authenticator port settings, go to "Configuring Authenticator Port Parameters" on page 357. To configure supplicant port settings, go to "Configuring Supplicant Port Parameters" on page 363.

Enabling or Disabling 802.1x Port-based Network Access Control

To enable or disable 802.1x Port-based Network Access Control, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 144 on page 354.
4. Click the **Enable Port Access** check box. A check in the box means the feature is activated on the switch. No check means the feature is disabled.

   For instructions on configuring the accounting feature, refer to “RADIUS Accounting” on page 369.
5. Click **Apply**.

   A change to the status of 802.1x Port-based Network Access Control is immediately implemented on the switch.
6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring Authenticator Port Parameters

To configure authenticator port parameters, perform the following procedure:

Note
The role of a port must be set to authenticator before the parameters can be configured. For instructions, refer to "Setting Port Roles" on page 354.

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 144 on page 354.
4. In the switch image, click the authenticator port to be configured. You can configure more than one authenticator port at a time. The selected port turns white.
5. Click **Settings**.

The Authenticator Parameters page is shown in Figure 146.

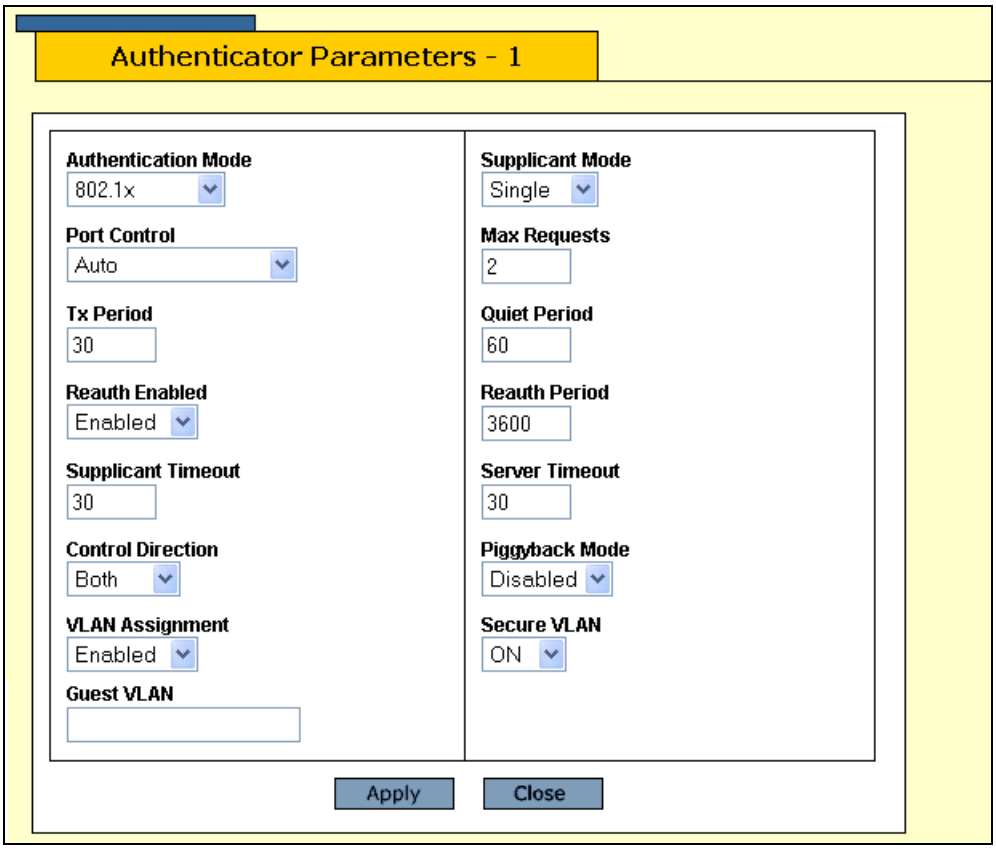

Figure 146. Authenticator Parameters Page

6. Configure the following parameters as needed:

   Authenticator Mode
   Sets the authenticator mode of an authenticator port. This parameter can take the following values:

   - **802.1x**: Specifies 802.1x username and password authentication. With this authentication method the supplicant must provide, either manually or automatically, a username and password to the authenticator port. This authentication method requires 802.1x client software on the supplicant nodes.
   - **MAC Based**: Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames received from a supplicant and automatically sends the address as both the username and password of the supplicant to the authentication server. Supplicant nodes do not need 802.1x client software for this authentication method.

Supplicant Mode
Sets the supplicant mode of an authenticator port. The possible settings are:

- **Single**: Configures the authenticator port to accept only one authentication. This mode should be used together with the piggy-back mode. When an authenticator port is set to the Single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port.
- **Multiple**: Configures the port to accept up to 20 authentications. Every client using an authenticator port in this mode must have a username and password combination.

Port Control
The possible settings are:

Auto - Activates 802.1x port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. This is the default setting.

Force-authorized - Disables IEEE 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.

Note
A supplicant connected to an authenticator port set to force-authorized must have 802.1x client software if the port's authenticator mode is 802.1x. Though the force-authorized setting prevents an authentication exchange, the supplicant must still have the client software to forward traffic through the port.

Force-unauthorized **-** Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

Max Requests
Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

TX Period
Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

Quiet Period
Sets the number of seconds that the port remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

Reauth Enabled
Controls whether the client must periodically reauthenticate. The default setting of enabled requires the client to periodically reauthenticate. The time period between reauthentications is set with the Reauth Period option. If this parameter is set to disabled, the client is not required to reauthenticate after the initial authentication, unless there is a change to the status of the link between the supplicant and the switch or the switch is reset or power cycled. The options are Enabled or Disabled. The default is Enabled.

Reauth Period
Specifies the time period in seconds between reauthentications of the client when the Reauth Enabled option is set to Enabled. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

Supplicant Timeout
Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Server Timeout
Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

Control Direction
Specifies how the port handles ingress and egress broadcast and multicast packets when in the unauthorized state. When a port is set to the Authenticator role, it remains in the unauthorized state until the client logs on by providing a username and password combination. In the unauthorized state, the port only accepts EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, are discarded until the supplicant has logged in. The options are:

Ingress - A port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client, but forwards all egress broadcast and multicast traffic to the same client.

Both - A port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the

client logs in. This is the default.

Piggyback Mode
Controls who can use the switch port in cases where there are multiple clients (e.g., the port is connected to an Ethernet hub). If set to enabled, the port allows all clients on the port to piggy-back onto the initial client's authentication. The port forwards all packets, regardless of the client, after one client has been authenticated. If set to Disabled, the switch port forwards only those packets from the client who was authenticated and discards packets from all other users.

VLAN Assignment
Controls whether an authenticator port uses the VLAN assignments returned by a RADIUS server. Options are:

- **Enabled**: Specifies that the authenticator port is to use the VLAN assignment returned by the RADIUS server when a supplicant logs on. This is the default setting. The port automatically moves to the designated VLAN after the supplicant successfully logs on.
- **Disabled**: Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even if the RADIUS server returns a VLAN assignment when a supplicant logs on. This is the default setting.

Secure VLAN
Controls the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode. Possible settings are:

- **On**: Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting.
- **Off**: Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

Guest VLAN
Specifies the VID of a Guest VLAN. The authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN. You can specify a Guest VLAN by either its name or VID. To remove a Guest VLAN without assigning a new one, delete the name or VID of the assigned VLAN.

7. Click **Apply**.

Changes to the authenticator settings are immediately implemented on a port.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Configuring Supplicant Port Parameters

To configure supplicant port parameters, perform the following procedure:

Note
The role of a port must be set to supplicant before the parameters can be configured. For instructions, refer to "Setting Port Roles" on page 354.

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 144 on page 354.
4. Click the supplicant port to be configured. You can configure more than one supplicant port at a time. The selected port turns white.
5. Click **Settings**.

   The Supplicant Parameters page is shown in Figure 146.

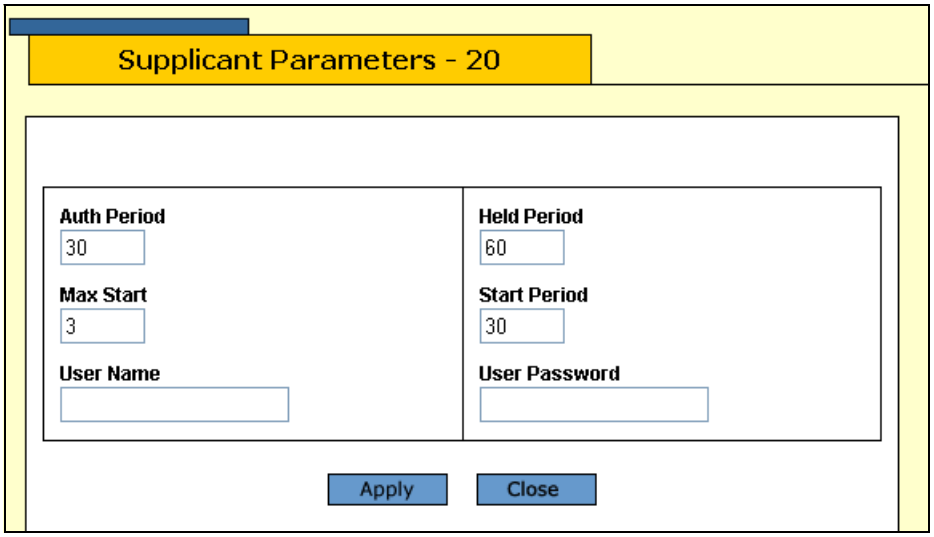

Figure 147. Supplicant Parameters Page

6. Configure the following parameters as needed:

   Auth Period
   Specifies the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 300 seconds. The default is 30 seconds.

Held Period
Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535 seconds. The default value is 60 seconds.

Max Start
Specifies the maximum number of times the supplicant sends EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

Start Period
Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

User Name
Specifies the username for the switch port. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case sensitive.

User Password
Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case sensitive.

7. Click **Apply**.

   Changes to the supplicant settings are immediately implemented on a port.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Port-based Network Access Control Parameters

You can display information about the port-based network access control status and settings of the ports on the switch. This section contains the following procedures:

- "Displaying the Port Status" (next)
- "Displaying the Port Settings" on page 367

Displaying the Port Status

To display the port-based network access control port status, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Network Security**.
3. Select the **802.1x Port Access** tab. The 802.1x Port Access tab is shown in Figure 148.

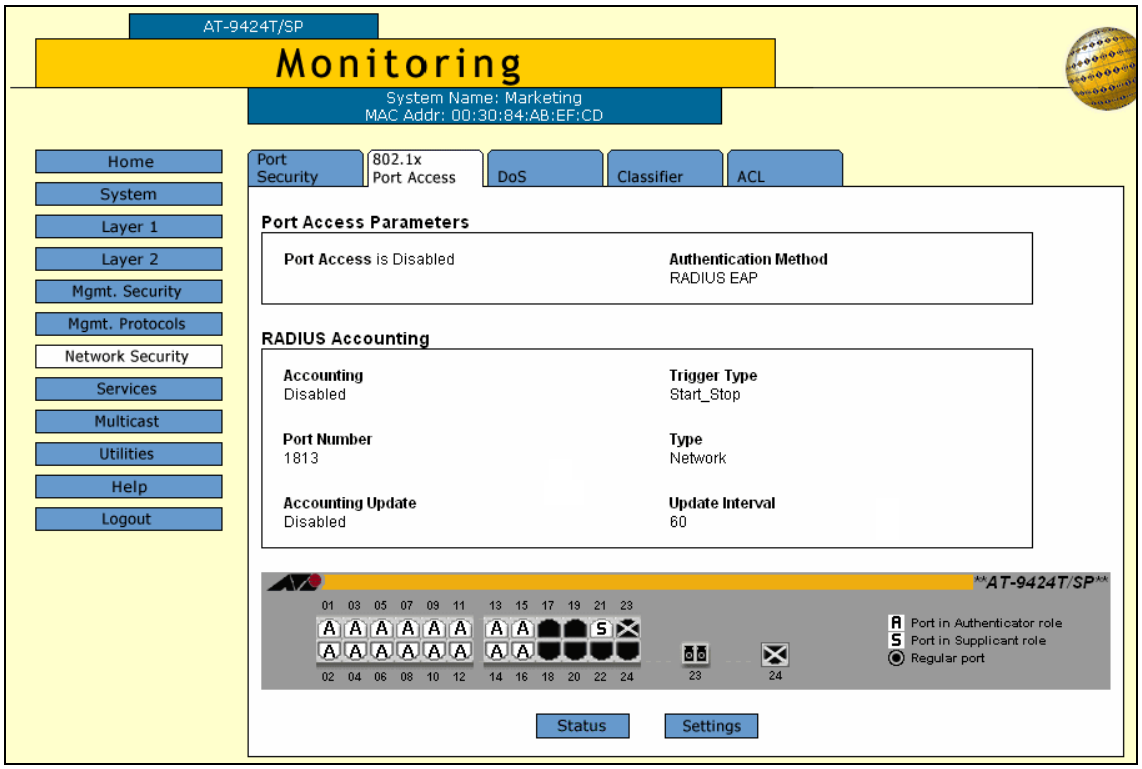

Figure 148. 802.1x Port Access Tab (Monitoring)

The image of the switch displays the roles of the ports. An "A" indicates an authenticator port and an "S" a supplicant port. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.

4. To see the status of the port, click the port and click **Status**. You can display the status of more than one port at a time.

   The Port Access Port Status page is shown in Figure 149.

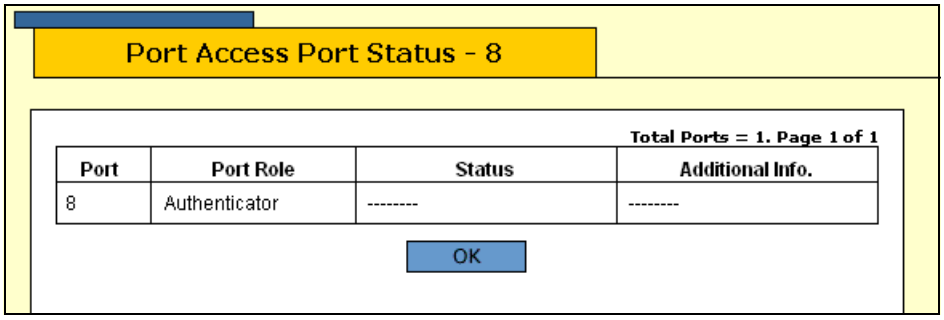

Figure 149. Port Access Port Status Page

The Port Access Port Status page displays a table that contains the following columns of information:

Port
Port number.

Port Role
Port access role configured for the port. The possible settings are None, Authenticator, or Supplicant.

Status
Status of the port. The status field is dependent on whether a port is configured as an authenticator or a supplicant.

The Status field can have the following values for an authenticator port:

Aborting
Authenticated
Authenticating
Connecting
Disconnected
Force_Auth
Force_Unauth
Held
Initialize

The Status field can have the following values for a supplicant port:

Acquired
Authenticated
Authenticating
Connecting
Disconnected
Held
Logoff

Additional Info
This field displays the MAC address of an authenticated node for authenticator ports with a status of Authenticated.

Displaying the Port Settings

To display the port settings for port-based network access control, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Network Security**.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 148 on page 365.
4. In the switch image, click a port and click **Settings**. You can display the settings of more than one port at a time.

Note
To view the settings of multiple ports, the selected ports must have the same port role (authenticator or supplicant).

The Authenticator Port Parameters page is displayed for authenticator ports, as shown in Figure 150.

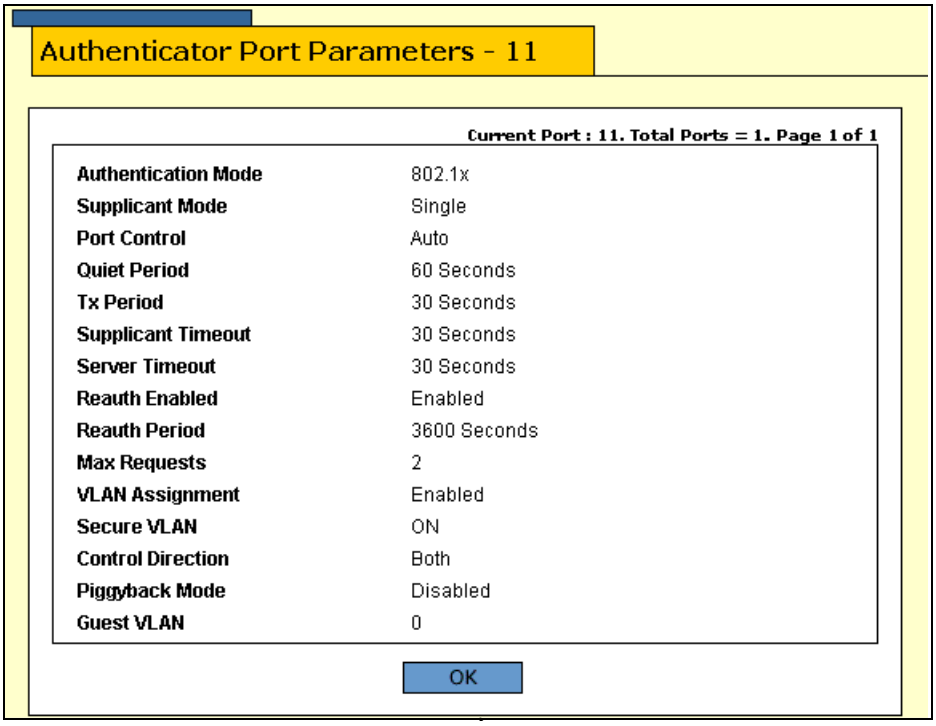

Figure 150. Authenticator Port Parameters Page

If you selected more than one authenticator port, the page includes a Next button. Use the button to scroll the page to view the settings of the other ports. For definitions of the authenticator port settings, refer to “Configuring Authenticator Port Parameters” on page 357.

The Supplicant Port Parameters Page is displayed for supplicant ports, as shown in Figure 151.

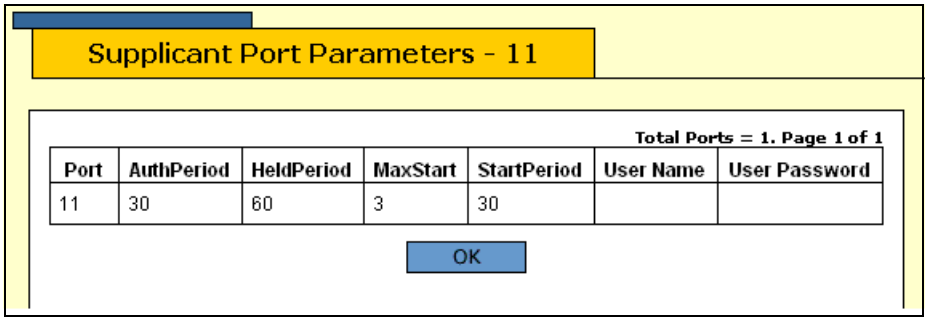

Figure 151. Supplicant Port Parameters Page

For definitions of the supplicant port settings, refer to “Configuring Supplicant Port Parameters” on page 363.

RADIUS Accounting

The AT-S63 Management Software supports RADIUS accounting for ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. For background information, refer to the *AT-S63 Management Software Features Guide*. This feature is disabled by default on the switch.

Configuring RADIUS Accounting

To configure RADIUS accounting, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab.

   The 802.1x Port Access tab is shown in Figure 144 on page 354
4. In the Configure RADIUS Accounting section, configure the following parameters as necessary.

   Enable Accounting
   Activates or deactivates RADIUS accounting on the switch. Select Enabled to activate the feature or Disabled to deactivate it. The default is Disabled.

   Trigger Type
   Specifies the action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

   Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

   Stop - The switch sends accounting information only when a client logs off.

   Port Number
   Specifies the UDP port for RADIUS accounting. The default is port 1813.

   Type
   Specifies the type of RADIUS accounting. The default is Network. You cannot change this value.

   Enable Update
   Controls whether the switch is to send interim accounting updates to the RADIUS server. A check in the box indicates that updating is enabled. No check in the box means that updating is disabled.

Update Interval
Specifies the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

5. Click **Apply**.

   Changes to the accounting settings are immediately implemented on the switch.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the RADIUS Accounting Settings

To display the RADIUS accounting settings, perform the following procedure:

1. From the home page, select **Monitoring**.
2. From the Monitoring menu, select the **Network Security** option.
3. Select the **802.1x Port Access** tab. The 802.1x Port Access tab is shown in Figure 148 on page 365.

   The RADIUS Accounting section provides the following information:

   Accounting
   The status of RADIUS accounting, either Enabled or Disabled.

   Trigger Type
   The action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

   Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

   Stop - The switch sends accounting information only when a client logs off.

   Port Number
   The UDP port for RADIUS accounting.

   Type
   The type of RADIUS accounting. The default is Network.

   Accounting Update
   Whether or not the switch sends interim accounting updates to the RADIUS server. The options are Enabled or Disabled.

   Update Interval
   The intervals, in seconds, at which the switch sends interim accounting updates to the RADIUS server.

Section VII

Management Security

This section has the following chapters:

- Chapter 24, “Encryption Keys, PKI, and SSL” on page 373
- Chapter 25, “Secure Shell (SSH)” on page 381
- Chapter 26, “TACACS+ and RADIUS Protocols” on page 387
- Chapter 27, “Management Access Control List” on page 399

Chapter 24

Encryption Keys, PKI, and SSL

This chapter explains how to view the encryption keys, PKI-based certificates, and SSL settings and includes the following sections:

- ❒ “Displaying the Encryption Keys” on page 374
- ❒ “Displaying the PKI Settings and Certificates” on page 376
- ❒ “Displaying the SSL Settings” on page 379

Note
You must use the menus or command line interface to configure encryption keys, PKI, and SSL.

Displaying the Encryption Keys

To configure the encryption keys, you must use the AT-S63 menus or command line interface. For more information about encryption keys, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the encryption keys, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Security** option.
3. Select the **Keys** tab.

   The Keys tab is shown in Figure 152.

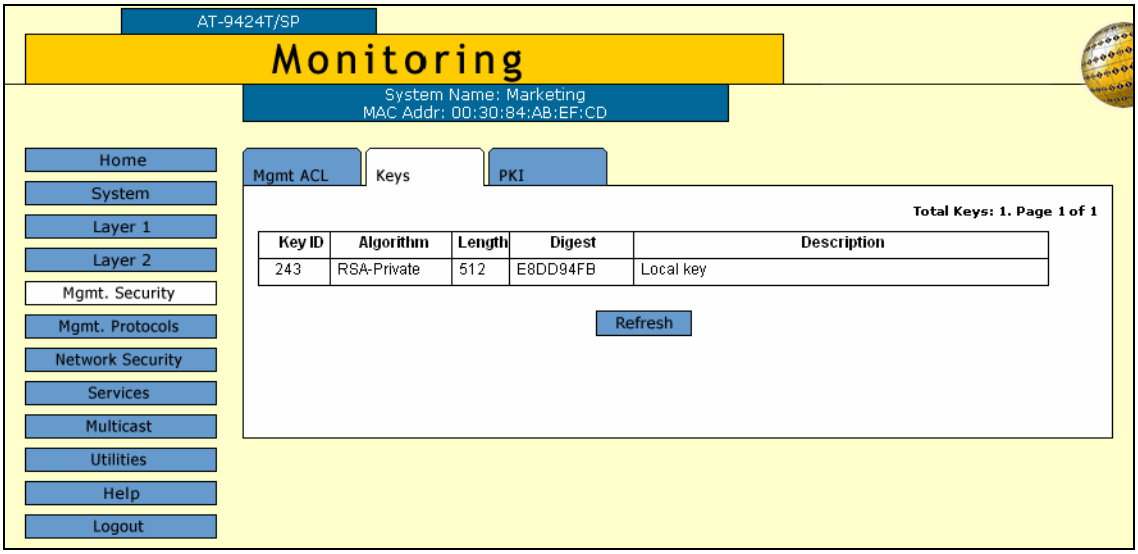

Figure 152. Keys Tab (Monitoring)

The Keys tab displays a table that contains the following columns of information:

ID
The identification number of the key.

Algorithm
The algorithm used in creating the encryption. This is always RSA - Private.

Length
The length of the key in bits.

Digest
The CRC32 value of the MD5 digest of the public key.

Description
The key's description.

You use these keys when you configure Secure Sockets Layer (SSL) or Secure Shell (SSH). To configure SSL you must use the AT-S63 menus or CLI interface. To configure SSH, refer to Chapter 25, "Secure Shell (SSH)" on page 381.

Displaying the PKI Settings and Certificates

You can view the current PKI settings and certificates on the switch. To configure the PKI settings and certificates, you must use the AT-S63 menus or command line interface. For more information about PKI, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the PKI settings and certificates, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Security** option.
3. Select the **PKI** tab.

   The PKI tab is shown in Figure 153.

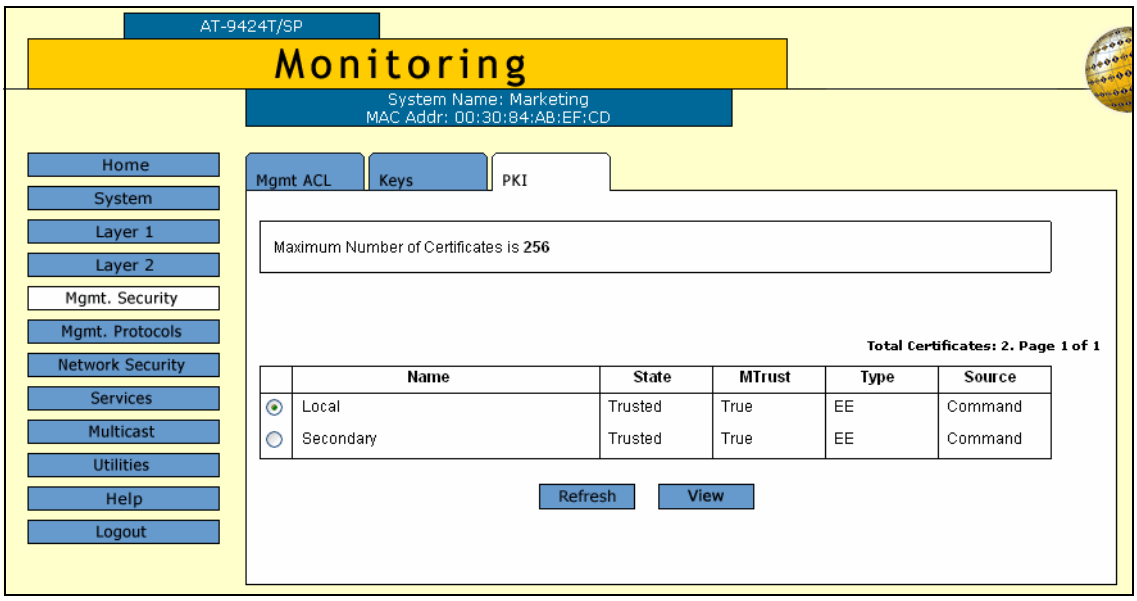

Figure 153. PKI Tab (Monitoring)

The upper section of the tab states the maximum number of certificates the certificate database can store. The default value is 256 certificates. The lower section displays a table that lists the current certificates in the database and contains the following columns of information:

Name
The certificate name.

State
The state of the certificate, one of the following:

Trusted - The certificate is from a trusted CA.

Untrusted - The certificate is from an untrusted CA.

MTrust (Manually Trusted)
The certificate has been manually verified that it is from a trusted or untrusted authority.

Type
The certificate type, one of the following:

EE - The certificate was issued by a CA.

CA - The certificate belongs to a CA.

Self - A self-signed certificate.

Source
The certificate was created on the switch.

4. To view the details about a certificate, click the certificate and click **View**.

   The X509 Certificate Details page is shown in Figure 154.

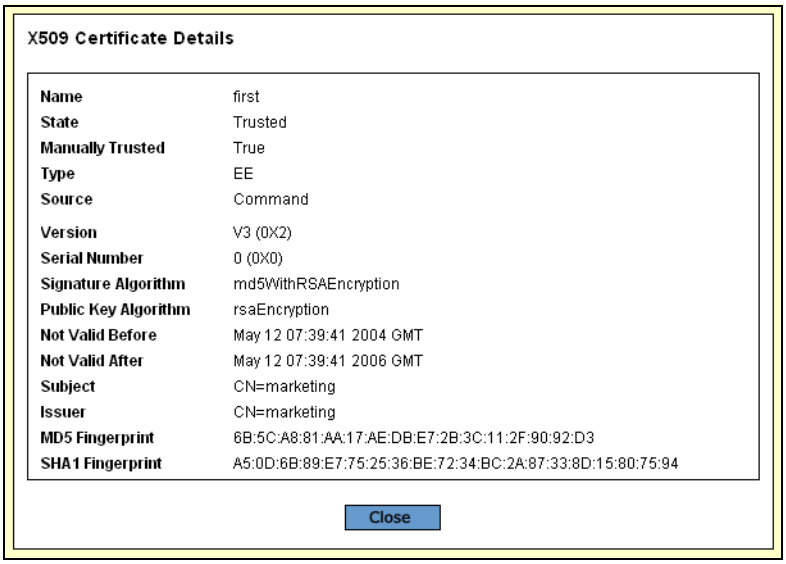

Figure 154. X509 Certificate Details Page

The X509 Certificate Details page provides the following information about the certificate:

Name
The name of the certificate.

State
Whether the certificate is Trusted or Untrusted.

Manually Trusted
Whether the certificate was manually trusted.

Type
The type of the certificate. The options are EE, SELF, and CA.

Source
The source of the certificate. The source for a self-signed certificate created by the switch is COMMAND.

Version
The version of X.509 that the certificate complies with.

Serial Number
The certificate's serial number.

Signature Algorithm
The algorithm used to sign the certificate.

Public Key Algorithm
The algorithm of the public key certified by the certificate.

Not Valid Before
The date the certificate became active.

Not Valid After
The date the certificate expires. Self-signed certificates are valid for two years.

Subject
The distinguished name of the subject of the certificate.

Issuer
The distinguished name of the issuer of the certificate.

MD5 Fingerprint
The MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint
The Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

5. Click **Close** to close the page.

Displaying the SSL Settings

To configure the SSL settings, you must use the AT-S63 menus or command line interface. For instructions, refer to the *AT-S63 Management Software Menus Interface User's Guide* and the *AT-S63 Management Software Command Line Interface User's Guide*.

To display the SSL settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Protocols** option.
3. Select the **SSL** tab.

   The SSL tab is shown in Figure 152.

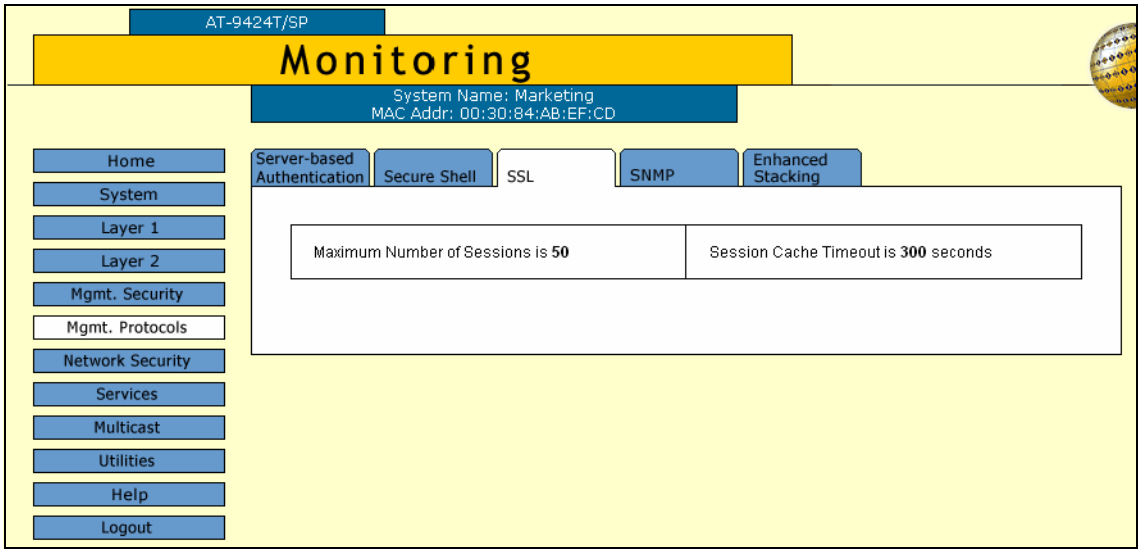

Figure 155. SSL Tab (Monitoring)

The SSL tab provides the following information:

Maximum Number of Sessions
The maximum number of SSL sessions allowed at one time.

Session Cache Timeout
The length of time before the session cache times out, in seconds.

Chapter 25

Secure Shell (SSH)

This chapter explains how to configure the Secure Shell (SSH) protocol and contains the following sections:

- ❒ “Configuring SSH” on page 382
- ❒ “Displaying the SSH Settings” on page 384

Configuring SSH

To configure SSH, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **Secure Shell** tab.

   The Secure Shell tab is shown in Figure 156.

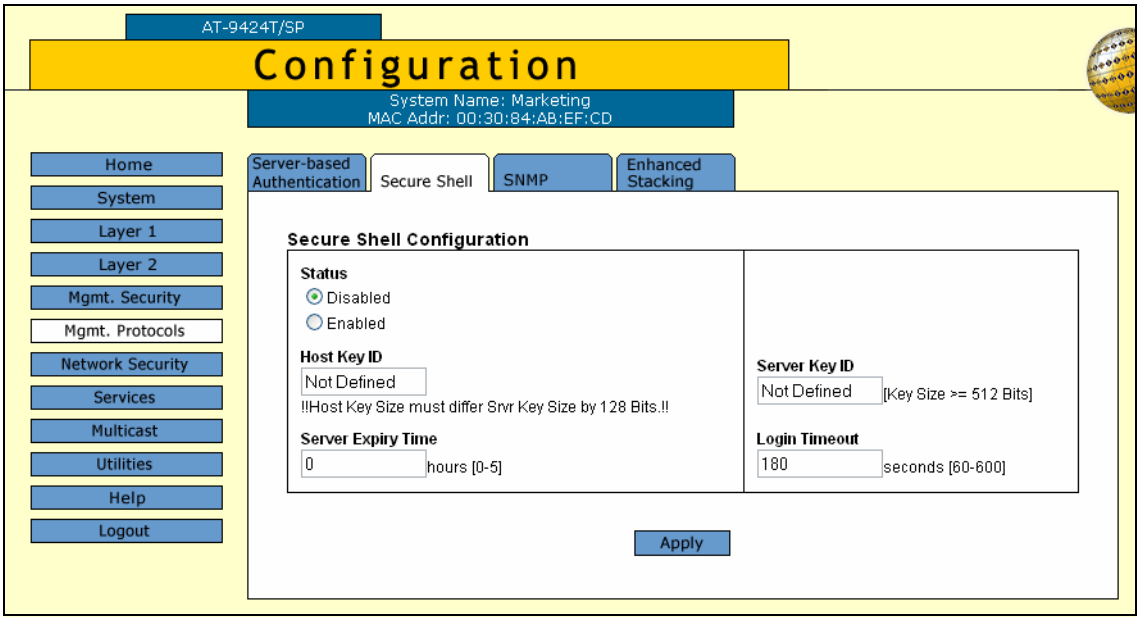

Figure 156. Secure Shell Tab (Configuration)

4. Configure the following parameters as necessary:

   Status
   Enables and disables the SSH server. The default is Disabled. SSH must be disabled to configure the protocol parameters.

   Note
   You cannot disable the SSH server when there is an active SSH connection.

   Host Key ID
   Specifies the ID number of the encryption key for the SSH host. The key must already exist on the switch. To view key ID numbers, refer to “Displaying the Encryption Keys” on page 374. The default is Not Defined.

Note
You cannot create encryption keys from the web browser interface, but you can from the menus and command line interfaces.

Server Key ID
Specifies the ID number of the encryption key for the SSH server. The key must already exist on the switch. The default is Not Defined.

Server Expiry Time
Sets the time, in hours, for a server key to expire. This timer determines how often a server key is regenerated for security purposes. A server key is only valid for the time period configured in the Server Key Expiry (Expiration) Time timer. Allied Telesis recommends setting this field to 1 to regenerate the key every hour.

Login Timeout
Specifies the time in seconds it takes to release the SSH server from an incomplete SSH client connection. The default is 180 seconds (3 minutes). The range is 60 to 600 seconds.

5. Click **Apply**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the SSH Settings

To view the Secure Shell settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.
3. Select the **Secure Shell** tab.

   The Secure Shell tab is shown in Figure 157.

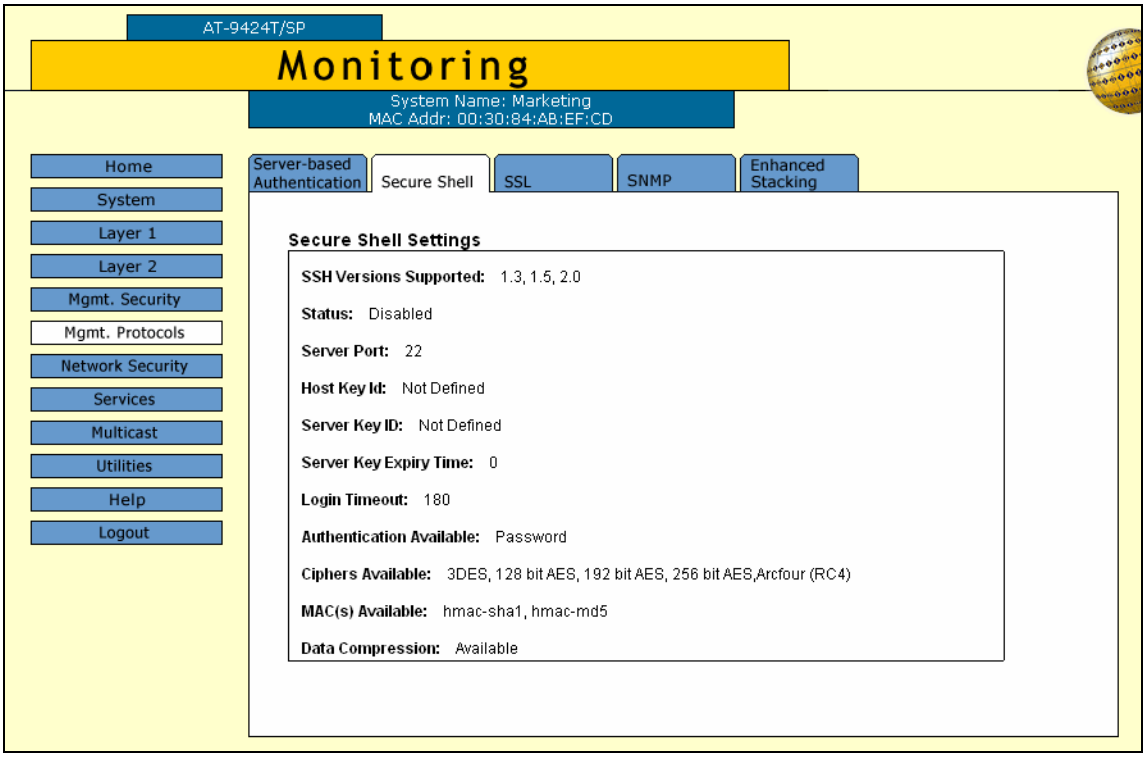

Figure 157. Secure Shell Tab (Monitoring)

The Secure Shell tab provides the following information:

SSH Versions Supported
The versions of SSH supported by the AT-S63 Management Software.

Status
Whether the SSH server is enabled or disabled.

Server Port
The well-known port number for SSH. The default is port 22.

Host Key ID
The encryption key ID of the host key.

Server Key ID
The encryption key ID of the server key.

Server Key Expiry Time
Length of time, in hours, until the server key is regenerated. The default is 0 hours which means the server key is not regenerated.

Login Timeout
Time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.

Authentication Available
Authentication method available. Currently, password authentication is the only supported method.

Ciphers Available
SSH ciphers that are available on the switch.

MAC(s) Available
Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.

Data Compression
Whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 26

TACACS+ and RADIUS Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedures:

- ❒ “Enabling or Disabling TACACS+ or RADIUS” on page 388
- ❒ “Configuring the TACACS+ Client Settings” on page 390
- ❒ “Displaying the TACACS+ Client Settings” on page 392
- ❒ “Configuring the RADIUS Client Settings” on page 394
- ❒ “Displaying the RADIUS Client Settings” on page 396

Enabling or Disabling TACACS+ or RADIUS

To enable or disable server-based authentication or to select a different authentication protocol, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Protocols** option.

   The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 158.

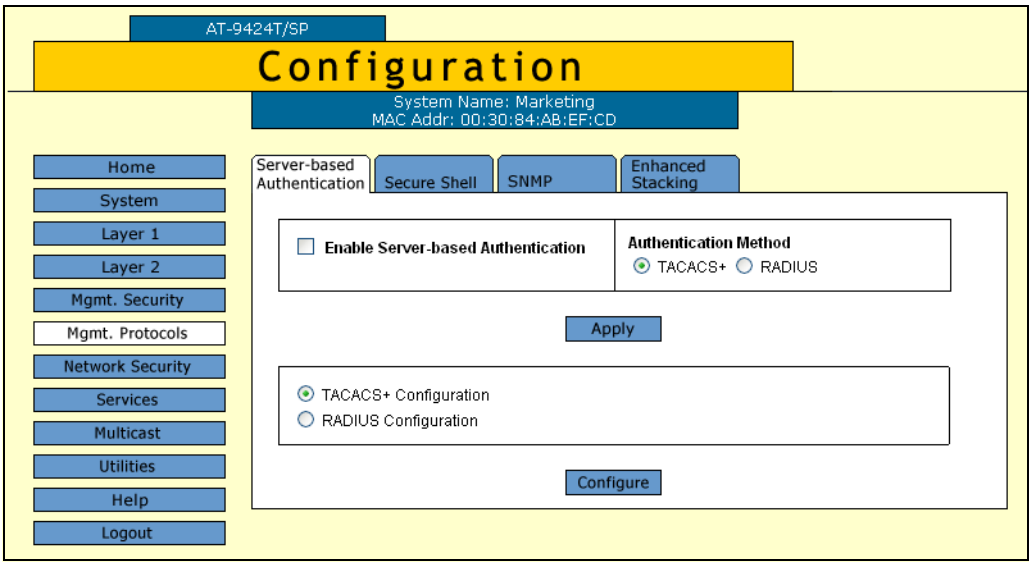

Figure 158. Server-based Authentication Tab (Configuration)

3. To select an authentication protocol, in the Authentication Method section of the tab, click either RADIUS or TACACS+. The default is TACACS+.

   Note
   The switch supports only one authentication protocol at a time. Furthermore, you cannot change to a different authenticator protocol when this feature is enabled.

4. To enable or disable the authentication feature, click the Enable Server-based Authentication check box. A check in the box indicates the feature is enabled. No check indicate the feature is disabled. The default is disabled.

Note
The Enable Server-based Authentication check box only applies to new TACACS+ or RADIUS manager accounts. If you are only using RADIUS for 802.1x port-based access control and not manager accounts, leave the check box empty. The switch can still access the RADIUS configuration information for 802.1x port-based access control.

5. Click **Apply**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

   To configure TACACS+, go to "Configuring the TACACS+ Client Settings" on page 390. To configure RADIUS, go to "Configuring the RADIUS Client Settings" on page 394.

Configuring the TACACS+ Client Settings

To configure the TACACS+ client, perform the following procedure:

1. From the home page, select **Configuration**.
2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 158 on page 388.
3. In lower section of the Server-based Authentication tab, click TACACS+ Configuration and click **Configure**.

   The TACACS+ Client Configuration page is shown in Figure 159.

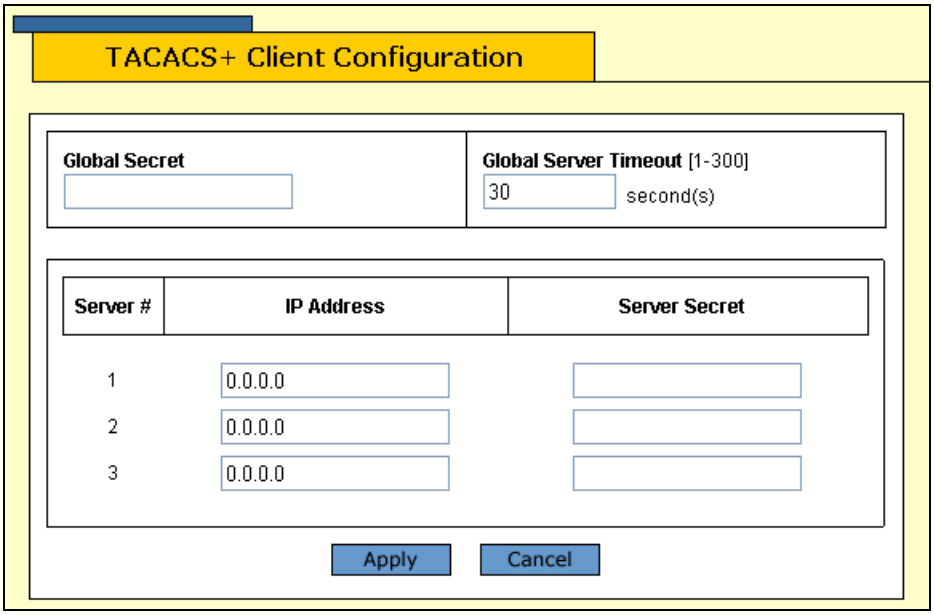

Figure 159. TACACS+ Client Configuration Page

4. Configure the following parameters as necessary.

   Global Secret
   Specify the global secret. If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address. The maximum key length is 39 characters.

   Global Server Timeout
   Specify the maximum amount of time the switch should wait for a response from a TACACS+ server. If the timeout expires without a response, the switch queries the next TACACS+ server in the list. If

there are no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and **Encryption Key**
Specify the IP addresses and encryption secrets of up to three TACACS+ servers. You can leave an encryption field blank if you entered the server's secret in the Global Secret field. The maximum length is 39 characters.

5. Click **Apply**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the TACACS+ Client Settings

To display the TACACS+ client settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 160.

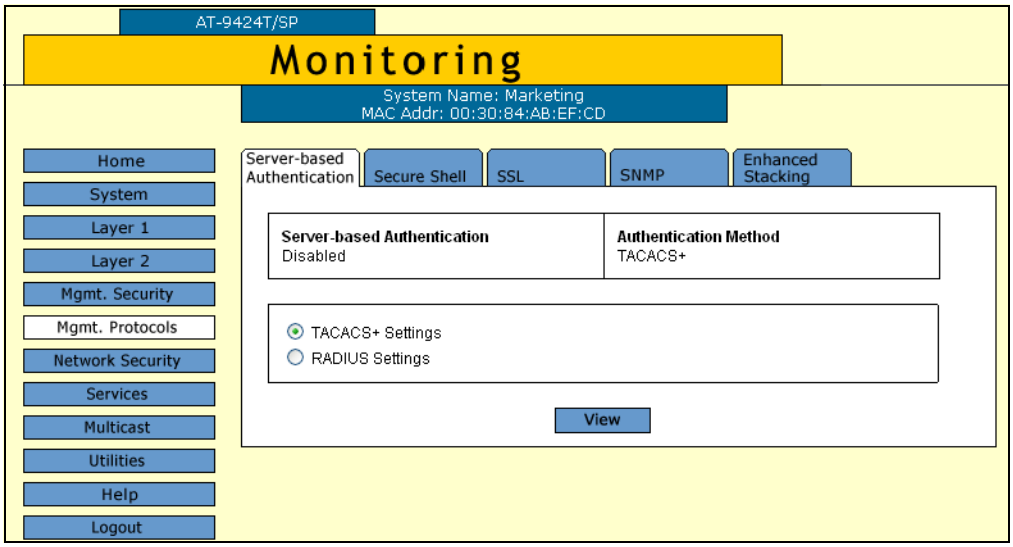

Figure 160. Server-Based Authentication Tab (Monitoring)

   The upper part of the page shows whether server-based authentication is enabled or disabled and the authentication method. The lower part of the page is used to view the settings of an authentication client.

3. In the lower portion of the tab, click TACACS+ Settings.
4. Click **View**.

The TACACS+ client configuration page is shown in Figure 161.

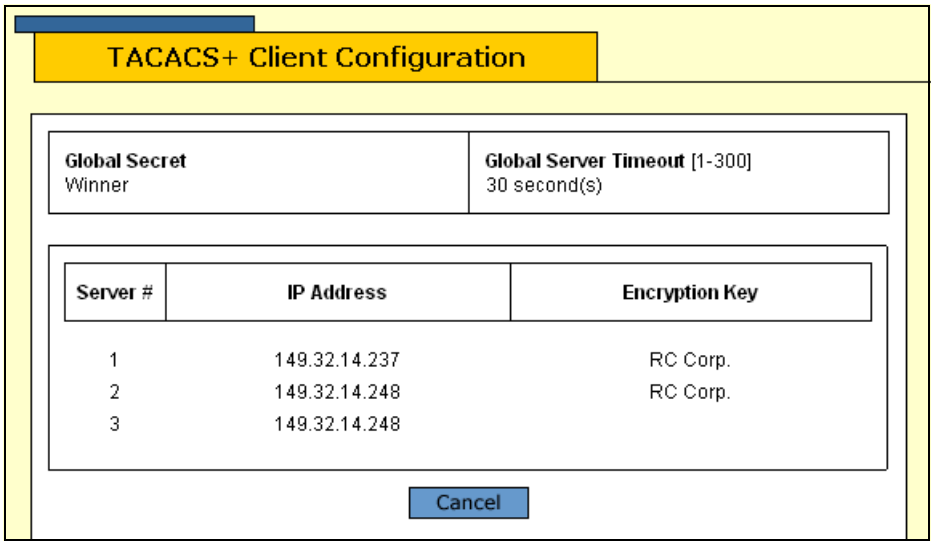

Figure 161. TACACS+ Client Configuration Page

The upper portion of the page provides the following information:

Global Secret
The TACACS+ server encryption secret.

Global Server Timeout
The maximum amount of time the switch waits for a response from a TACACS+ server.

The lower portion of the page displays a table with the following columns of information:

Server #
The server number, one of three.

IP Address
IP addresses of up a network server containing TACACS+ server software.

Encryption Key
Encryption key for the server. This parameter is blank if the key is specified in the global secret.

Configuring the RADIUS Client Settings

To configure the RADIUS client, perform the following procedure:

1. From the home page, select **Configuration**.
2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 158 on page 388.
3. In lower section of the Server-based Authentication tab, click RADIUS Configuration and click **Configure**.

   The RADIUS Client Configuration page is shown in Figure 159.

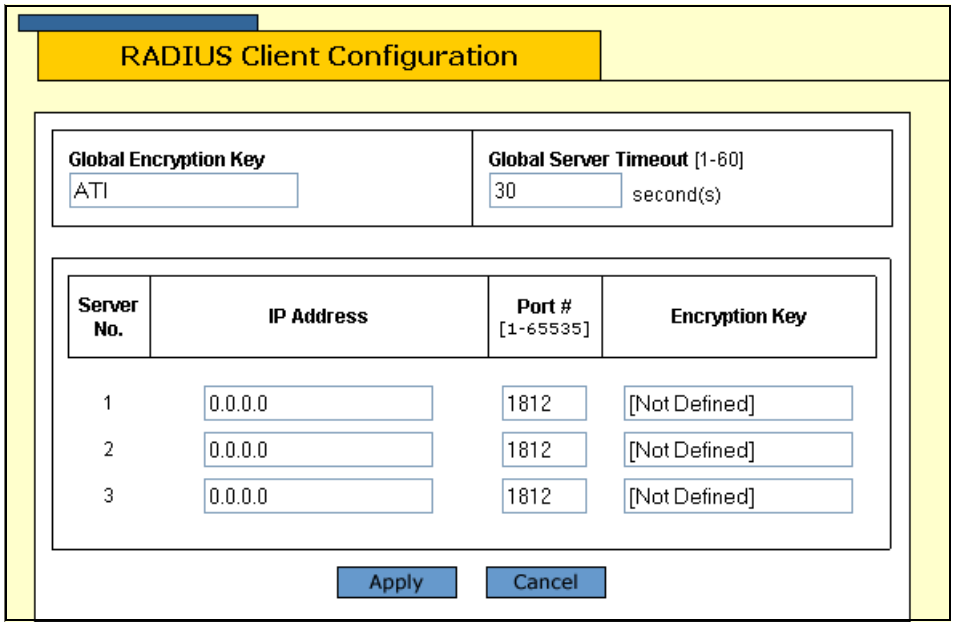

Figure 162. RADIUS Client Configuration Page

4. Configure the following parameters as necessary.

   Global Encryption Key
   Specify the global encryption key. If all of the RADIUS servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify the keys with the servers' IP addresses. The maximum key length is 39 characters.

   Global Server Timeout
   Specify the maximum amount of time the switch should wait for a response from a RADIUS server. If the timeout expires without a response, the switch queries the next RADIUS server in the list. If

there are no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and **Encryption Key**
Specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to three servers. You can leave the encryption field blank for a server if you entered the server's key in the Global Encryption Key field. The maximum length of the encryption key is 39 characters.

5. Click **Apply**.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the RADIUS Client Settings

To display the RADIUS client settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. Select the **Mgmt. Protocols** option.

   The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 160 on page 392.

   The upper part of the page shows whether server-based authentication is enabled or disabled and the authentication method. The lower part of the page is used to view the settings of an authentication client.
3. In the lower portion of the page, click **RADIUS Settings**.
4. Click **View**.

   The RADIUS Client Configuration page is shown in Figure 161.

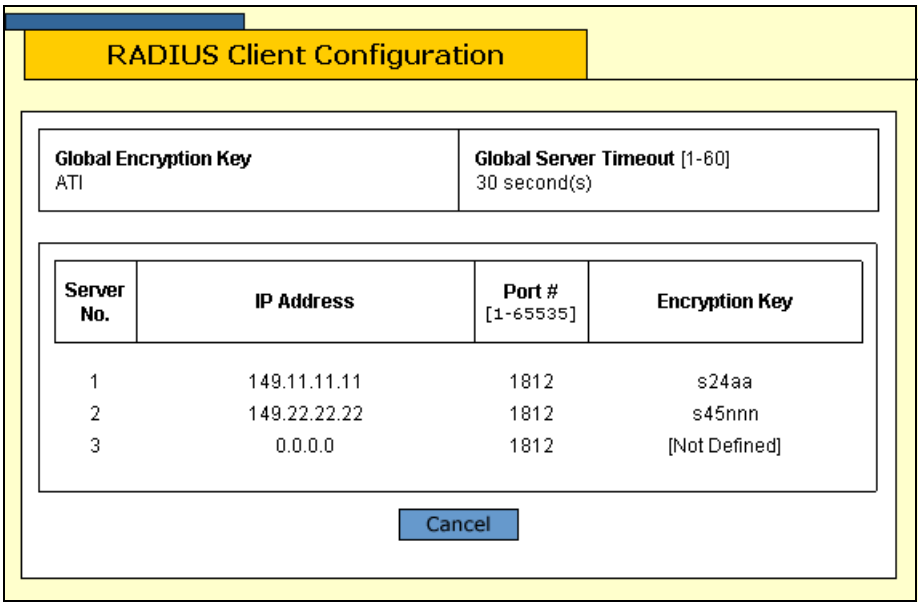

Figure 163. RADIUS Client Configuration Page

The upper portion of the page displays the following information:

Global Encryption Key
The global encryption secret.

Global Server Timeout
Specifies the maximum amount of time the switch waits for a response from a RADIUS server.

The lower portion of the page displays a table that contains the following columns of information:

Server #
Specifies the server number, one of three.

IP Address
Specifies the IP address of the RADIUS server.

Port
Specifies the port of the RADIUS server.

Encryption Key
Specifies the encryption key for that server. This parameter is blank if the key is specified in the Global Encryption Key field.

Chapter 27

Management Access Control List

The management access control list (ACL) enhances security of the switch by restricting Telnet and web browser management access. The sections in this chapter include:

- ❒ “Enabling or Disabling the Management ACL” on page 400
- ❒ “Creating an ACE” on page 402
- ❒ “Modifying an ACE” on page 404
- ❒ “Deleting an ACE” on page 405
- ❒ “Displaying the Management Access Control List” on page 406

Enabling or Disabling the Management ACL

This procedure enables and disables the management ACL. When the management ACL is enabled, remote Telnet and web browser management of the switch is restricted to just those management stations specified by the access control entries in the ACL. When the feature is disabled, any remote management workstation can access the switch.

Note
Do not activate the management ACL until you have specified the access control entries (ACEs). Otherwise, it will be impossible to remotely manage the unit from a Telnet or web browser management session because the switch will discard all remote management packets. For instructions on how to add ACEs, refer to “Creating an ACE” on page 402.

To enable or disable the management ACL, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Security** option.
3. Select the **Mgmt. ACL** tab.

   The tab is shown in Figure 164.

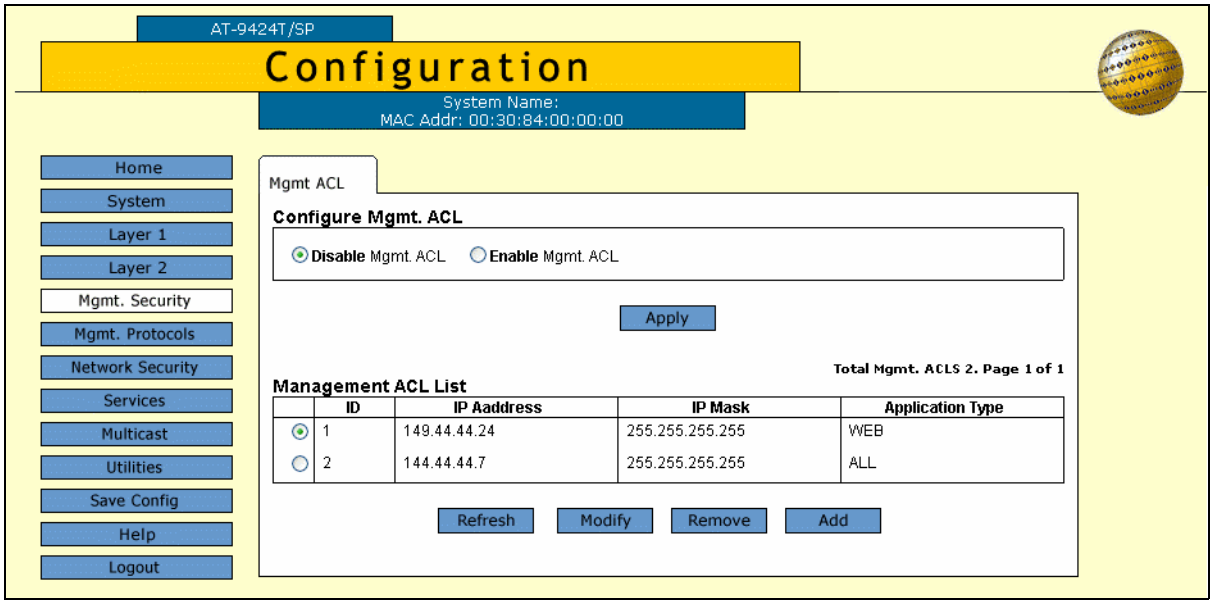

Figure 164. Mgmt. ACL Tab (Configuration)

The table in the Management ACL List lists the existing ACEs on the switch. The bottom portion is used to add entries, as explained in "Creating an ACE" on page 402.

4. Click either **Enable MGMT**. **ACL** or **Disable MGMT**. **ACL**. The default setting is disabled.

5. Click **Apply**.

   The new status of the management ACL is immediately activated on the switch.

   Note
   Your management session will immediately end and you will not be able to reestablish it if you activate the feature without an ACE that identifies your management station. To recover, establish a local management session on the switch and deactivate the feature or create an ACE that identifies the remote management station.

6. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Creating an ACE

To add a new ACE to the management ACL, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Security** option.
3. Select the **Mgmt. ACL** tab.

   The tab is shown in Figure 164 on page 400.
4. To add a new ACE, click **Add**.

   The Add New MACL page is shown in Figure 165.

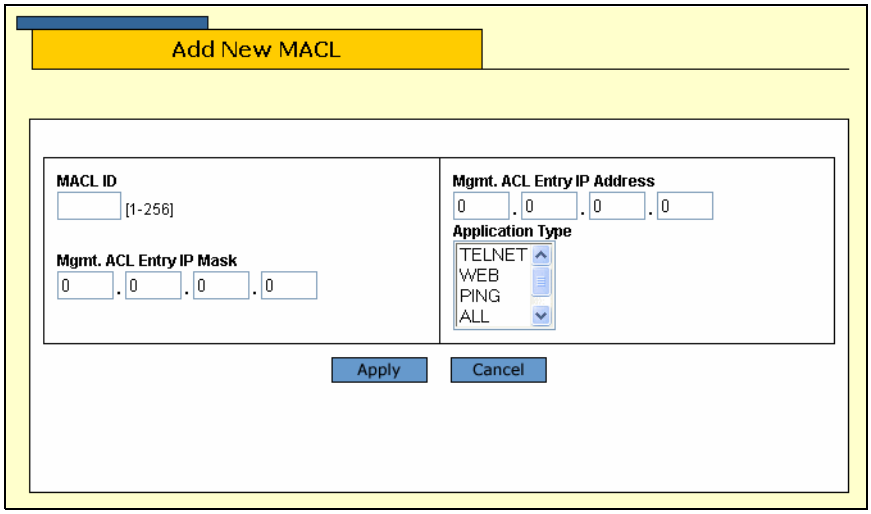

Figure 165. Add New MACL Page

5. Configure the following parameters in the Add New MACL page:

   MACL ID
   Specifies an identification number for the access control entry. Every ACE must have a unique number. The range is 1 to 256.

   Mgmt. ACL Entry IP Address
   Specifies the IP address of a management workstation to be allowed management access to the switch (for example, 149.11.11.11). Alternatively, you can specify a subnet. You must enter an IP address. If you enter an IP address of a specific management node, that node will be permitted remote management access to the switch. If you enter a subnet, any management node in the subnet will be permitted remote management access to the switch.

Mgmt. ACL Entry IP Mask
Specifies a mask that indicates the parts of the IP address the switch should filter on. A binary "1" indicates the switch should filter on the corresponding bit of the address, while a "0" indicates that it should not. If you are filtering on a specific IP address, use the mask 255.255.255.255. If you are filtering on a subnet, the mask will depend on the address. For example, to allow all management workstations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.

Application
Specifies the application the management station can use to manage the switch. You can select more than one by holding down the Shift key when making the selections. The options are:

Telnet - Allows Telnet management.

Web - Allows web browser management.

Ping - Allows the management workstation to ping the switch.

All - Allows all of the above.

6. Click **Apply**.

   The new ACE is added to the table in the middle section of the tab.

7. If desired, repeat Steps 4 and 6 to add more ACEs to the Management ACL.

8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Modifying an ACE

To modify an ACE, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Security** option.
3. Select the **Mgmt. ACL** tab.

   The tab is shown in Figure 164 on page 400.
4. Select the ACE to be modified from the Management ACL List section in the tab and click **Modify**.

   The Modify MACL page is shown in Figure 166.

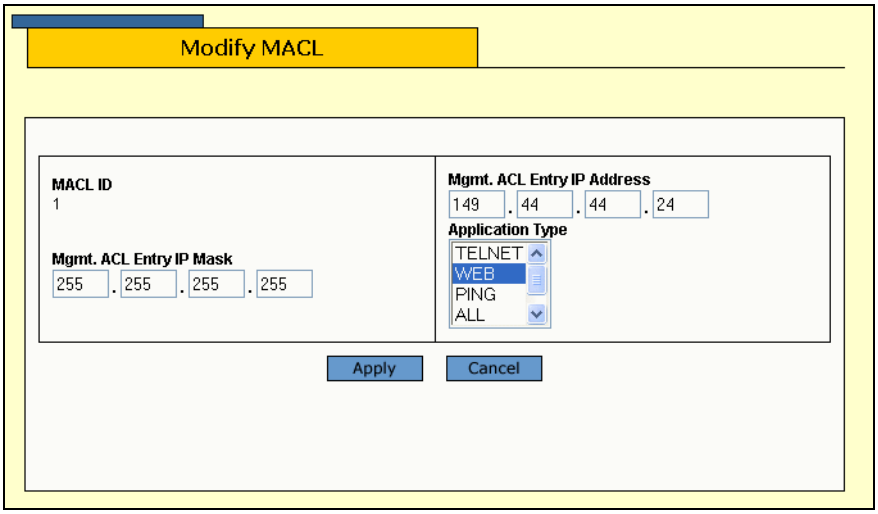

Figure 166. Modify MACL Page

5. Change the parameters in the Add New MACL page, as necessary. For parameter definitions, refer to “Creating an ACE” on page 402. The ID number of an entry cannot be changed.
6. Click **Apply**.

   The changes are immediately activated on the ACE.
7. If desired, repeat Steps 4 to 6 to modify more ACEs.
8. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Deleting an ACE

To delete an ACE from the Management ACL, perform the following procedure:

1. From the home page, select **Configuration**.
2. From the Configuration menu, select the **Mgmt. Security** option.
3. Select the **Mgmt. ACL** tab.

   The tab is shown in Figure 164 on page 400.
4. Select the ACE to be deleted from the Management ACL List section in the tab and click **Remove**.

   The ACE is deleted from the switch.
5. To permanently save your changes, select the **Save Config** option in the Configuration menu.

Displaying the Management Access Control List

To display the management access control list and its access control entries, perform the following procedure:

1. From the home page, select **Monitoring**.
2. From the Monitoring menu, select the **Mgmt. Security** option.
3. Select the **Mgmt ACL** tab.

   The Mgmt. ACL tab is shown in Figure 167.

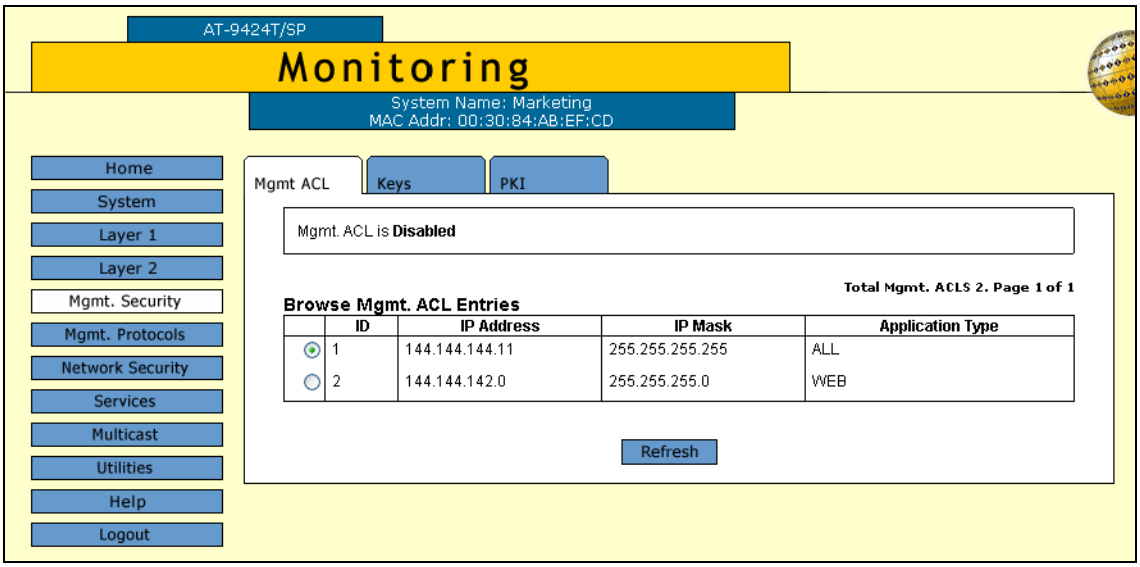

Figure 167. Mgmt. ACL Tab (Monitoring)

The top section of the tab displays the status of the Management ACL as enabled or disabled. The bottom section lists the existing ACEs. For definitions of the columns, refer to “Creating an ACE” on page 402.

Index

Numerics

802.1x Port-based Network Access Control
- access role, configuring 354
- authenticator port, configuring 357
- configuring 354
- disabling 356
- enabling 356
- port parameters, displaying 367
- port role, configuring 354
- port status, displaying 365
- supplicant port, configuring 363

A

active boot configuration file, setting 109
administrator name
- configuring 29

aging time
- changing 83

app (applicant state machine) 339
AT-S63 software
- resetting to factory defaults 37

auth period 363
authentication protocols, enabling or disabling 388
automatic port security level 349
autonegotiation, configuring 46

B

back pressure
- configuring 48

boot configuration file 109
bridge forwarding delay
- Multiple Spanning Tree Protocol (MSTP) 298
- Rapid Spanning Tree Protocol (RSTP) 286
- Spanning Tree Protocol (STP) 278

bridge hello time
- Multiple Spanning Tree Protocol (MSTP) 298
- Rapid Spanning Tree Protocol (RSTP) 286
- Spanning Tree Protocol (STP) 278

bridge identifier
- Rapid Spanning Tree Protocol (RSTP) 286
- Spanning Tree Protocol (STP) 279

bridge max age
- Multiple Spanning Tree Protocol (MSTP) 298
- Rapid Spanning Tree Protocol (RSTP) 286
- Spanning Tree Protocol (STP) 278

bridge priority
- Rapid Spanning Tree Protocol (RSTP) 285
- Spanning Tree Protocol (STP) 277

bridge protocol data unit (BPDU) 286

C

ciphers available parameter 385
CIST priority parameter 299
Class of Service (CoS)
- configuring 156
- mapping to egress queues 158
- schedule, displaying 163
- scheduling, configuring 160
- settings, displaying 161

Common and Internal Spanning Tree (CIST), configuring 299
community name
- SNMPv3 protocol 255, 258

CoS. *See* Class of Service (CoS)

D

data compression parameter 385
daylight savings time (DST) 34
Denial of Service (DoS) defense
- configuring 188
- enabling or disabling 190
- mirror port 190
- settings, displaying 191

document conventions 21
DoS. *See* Denial of Service (DoS) Defense
duplex mode
- configuring 47

E

edge port
- Multiple Spanning Tree Protocol (MSTP) 307

encryption keys, displaying 374
enhanced stacking
- changing switches 60
- configuring 58
- setting switch status 58

event log
- clearing 126
- disabling 120
- displaying 122
- enabling 120
- modifying full action 127
- saving to a file 128
- severity codes 125
- software module list 123

F

factory defaults
  resetting switch 37
flash memory, displaying files in 106
flow control
  configuring 48
flow group
  configuring 166
  deleting 170
  displaying 170
  modifying 169
force version
  Multiple Spanning Tree Protocol (MSTP) 298
  Rapid Spanning Tree Protocol (RSTP) 285

G

GARP VLAN Registration Protocol (GVRP)
  configuration, displaying 335
  configuring 332
  counters, displaying 341
  database, displaying 337
  disabling 334
  enabling 334
  GIP connected ports ring, displaying 344
  GVRP state machine, displaying 338
  port configuration, displaying 336
global encryption key
  configuring 394, 396
global secret
  configuring 390, 393
global server timeout
  configuring 390, 393
GVRP. *See* GARP VLAN Registration Protocol (GVRP)

H

hardware information 40
held period 364
hello time
  Rapid Spanning Tree Protocol (RSTP) 286
  Spanning Tree Protocol (STP) 278
host key ID parameter 382
host nodes, displaying 197
host/router timeout interval
  configuring 195

I

IGMP. *See* Internet Group Management Protocol (IGMP) Snooping
Internet Group Management Protocol (IGMP) snooping
  configuring 194
  disabling 194
  enabling 194
intrusion action 350
intrusion action (port)
  configuring 352

L

limited port security level 349
local interface
  displaying IP address 39
locked port security level 349
login timeout parameter 383

M

MAC address aging time
  changing 83
MAC address table, displaying 76
MAC addresses
  adding 79
  deleting dynamic 82
  deleting multicast 81
  displaying 76
MACs available parameter 385
management access control list
  adding an ACE 402
  deleting an ACE 405
  disabling 400
  enabling 400
  modifying an ACE 404
management access levels 30
manager access 30
manager password
  configuring 30
master switch
  assigning 58
  defined 58
  returning to 62
max age
  Rapid Spanning Tree Protocol (RSTP) 286
  Spanning Tree Protocol (STP) 278
max hops, Multiple Spanning Tree Protocol (MSTP) 299
max requests 359
max start 364
maximum multicast groups
  configuring 195
MCHECK 287, 306
MDI/MDIX mode 47
MSTI ID
  creating 300
  deleting 302
  modifying 301
MSTP. *See* Multiple Spanning Tree Protocol (MSTP)
multicast groups, maximum
  configuring 195
multicast host topology
  configuring 194
multicast MAC address
  adding 79
  deleting 81
  displaying 76
multicast router ports
  configuring 195
multicast routers, displaying 199

Multiple Spanning Tree Protocol (MSTP)
bridge forwarding delay 298
bridge hello time 298
bridge max age 298
bridge settings, configuring 296
configuration name 298
configuring 296
disabling 294
edge port 307
enabling 294
force version 298
max hops 299
parameters, configuring 296
point-to-point port 306
port external path cost 306
port internal path cost 305
port parameters
configuring 304
displaying 308
port priority 305
port status, displaying 308
resetting to defaults 313

O

operator access 30
operator password
configuring 30

P

password
changing 30
piggyback mode 361
pinging 36
PKI certificates
displaying 376
PKI certificates, displaying 376
PKI. *See* Public Key Infrastructure (PKI)
point-to-point port
Multiple Spanning Tree Protocol (MSTP) 306
Rapid Spanning Tree Protocol (RSTP) 288
policy
configuring 180
deleting 184, 185
displaying 185
modifying 183
port
configuring parameters, basic 44
disabling 46
enabling 46
resetting to defaults 56
statistics, displaying 53
status
displaying 51
port control
802.1x port-based access control 359
force-authorized 359
force-unauthorized 359
port cost
Multiple Spanning Tree Protocol (MSTP) 305
Rapid Spanning Tree Protocol (RSTP) 287
Spanning Tree Protocol (STP) 280
port mirror
creating 96
deleting 101
disabling 100
displaying 102
modifying 99
port parameters, configuring
basic 44
Multiple Spanning Tree Protocol (MSTP) 296
Rapid Spanning Tree Protocol (RSTP) 284
Spanning Tree Protocol (STP) 276
port participating parameter 350
port priority
Multiple Spanning Tree Protocol (MSTP) 305
Rapid Spanning Tree Protocol (RSTP) 287
Spanning Tree Protocol (STP) 279
port security
displaying 351
intrusion action 352
port security levels, MAC 349
port speed
configuring 46
port trunk
creating 86
deleting 92
displaying 93
modifying 90
port-based access control. *See* 802.1x Port-based Network Access Control
port-based VLAN
creating 318
deleting 325
displaying 327
modifying 323
Public Key Infrastructure (PKI)
settings, displaying 376

Q

QoS. *See* Quality of Service (QoS)
Quality of Service (QoS)
See also traffic class, flow group, and policy 165
quiet period, configuring 360

R

RADIUS
configuring 394
disabling 388
displaying settings 396
enabling 388
server timeout 397
RADIUS accounting
configuring 369
settings, displaying 370
RADIUS server
encryption secret 395
encryption secret, configuring 391
IP address, configuring 395

Rapid Spanning Tree Protocol (RSTP)
bridge forwarding delay 286
bridge hello time 286
bridge identifier 286
bridge max age 286
bridge priority 285
bridge settings, configuring 284
disabling 274, 294
edge port, configuring 288
enabling 274, 294
force version 285
MCHECK 287, 306
point-to-point port, configuring 288
port cost 287
port priority 287
port settings, displaying 288
resetting to defaults 291
reauth period, configuring 360
reg (registrar state machine) parameter 340
RSTP. *See* Rapid Spanning Tree Protocol (RSTP)

S

Secure Shell (SSH) protocol
configuring 382
displaying settings 384
Secure Sockets Layer (SSL)
displaying settings 379
secured port security level 349
server authentication UDP port
configuring 395
server key ID parameter 383
server timeout, configuring 360
session cache timeout
configuring 379
Simple Network Time Protocol (SNTP)
configuring 32
servers 32
slave switch
assigning 58
defined 58
SNMP management
disabling 66
enabling 66
SNMPv1 and SNMPv2c community
creating 68
deleting 72
displaying 73
modifying 71
SNMPv3 Access Table entry
creating 222
deleting 225
displaying 263
modifying 226
SNMPv3 community name, modifying 258
SNMPv3 Community Table entry
creating 254
deleting 257
displaying 268
modifying 257
SNMPv3 Notify Table entry
creating 235
deleting 237
displaying 265
modifying 238
SNMPv3 SecurityToGroup Table entry
creating 229
deleting 232
displaying 264
modifying 232
SNMPv3 Target Address Table entry
creating 240
deleting 243
displaying 266
modifying 244
SNMPv3 Target Parameters Table entry
creating 247
deleting 250
displaying 267
modifying 251
SNMPv3 User Table entry
creating 208
deleting 211
displaying 260
modifying 212
SNMPv3 View Table entry
creating 216
deleting 219
displaying 262
modifying 219
SNTP. See Simple Network Time Protocol (SNTP)
software information 40
Spanning Tree Protocol (RSTP)
parameters, displaying 280
Spanning Tree Protocol (STP)
bridge forwarding delay 278
bridge hello time 278
bridge identifier 279
bridge max age 278
bridge parameters, configuring 276
bridge priority 277
disabling 274, 294
enabling 274, 294
parameters, displaying 280
port cost 280
port priority 279
resetting to defaults 282
SSH. *See* Secure Shell (SSH)
SSL. *See* Secure Sockets Layer (SSL)
static MAC address
adding 79
deleting 81
static unicast MAC address, displaying 76
STP ID 344
STP. *See* Spanning Tree Protocol (STP)
supplicant port, start period 364
supplicant timeout 360
switch
hardware information 40

software information 40
switch name, configuring 28
switch, rebooting 35
system date
setting 32
system file
downloading 112
uploading 116
system name
configuring 29
system time
setting 32

T

TACACS+
configuring 390
disabling 388
displaying settings 392
enabling 388
server timeout
configuring 394
tagged VLAN
creating 318
deleting 325
displaying 327
modifying 323
threshold 350
traffic class
configuring 172
deleting 178
displaying 178
modifying 177
tx period, configuring 360

U

unavailable status, defined 58
uplink port
configuring 326
displaying 319, 328
user name
configuring 364
user password, configuring 364

V

versions supported (SSH) parameter 384
virtual LAN (VLAN)
creating 318
deleting 325
displaying 327
mode, selecting 326
modifying 323
VLAN type
port-based or tagged VLAN 321